

# **The Interplay of Web Aggregation and Regulations (LawTech)**

Harry Zhu, Stuart Madnick, Michael Siegel

CISL WP #02-17  
November 2002

**MIT Sloan School of Management  
50 Memorial Drive  
Cambridge, Massachusetts 02142-1347**

# THE INTERPLAY OF WEB AGGREGATION AND REGULATIONS

Hongwei Zhu, Stuart E. Madnick, Michael D. Siegel  
MIT Sloan School of Management  
30 Wadsworth Street  
Cambridge, MA 02142, USA  
{mrzhu, smadnick, msiegel}@mit.edu

## ABSTRACT

The development of web technology has led to the emergence of web aggregation, a service that collects existing web data and turns them into more useful information. We review the development of both comparison and relationship aggregation and discuss their impacts on various stakeholders.

The aggregator's capability of transparently extracting web data has raised challenging issues in database and privacy protection. Consequently, new regulations are introduced or being proposed. We analyze the interactions between aggregation and related policies and provide our insights about the implications of new policies on the development of web aggregation.

## KEY WORDS

International IP Law, Privacy Law, Web Aggregation

## 1. Introduction

The development of Information Technology (IT) and the Internet over the past decade has brought sweeping social and economic changes to our society. Conversely, new regulations in response to emerging IT enabled services have great impact on their effectiveness and evolution. We will examine the interplay between IT and policy using the example of web aggregation.

The web has dual effects on the dissemination of information. It allows information creators to directly reach vast end users, eliminating the intermediaries necessary in traditional media. Meanwhile, since no single information creator can meet all the information needs of a user and there are over 40 million potentially useful sources in the U.S. alone<sup>1</sup>, there is a need for intermediaries to bring information from various sources to end users. This latter effect has been the major motivation for the emergence and the development of web aggregation.

Web aggregation is a service that transparently collects information from multiple web sources and performs useful analysis to add value to the integrated information [1]. Shopbots, such as DealTime.com and Kelkoo.com, are examples of comparison aggregation, which allow users to compare prices and other attributes of products offered by multiple vendors. Relationship aggregation allows users to manage multiple relationships using a single logon. For example, Citigroup's mycity.com allows users to view all their online relationship accounts in one place. We will discuss in detail the evolution and impact of both comparison and relationship aggregation in section 2.

Since aggregation service involves multiple information creators, and especially relationship aggregation deals with personal information, complicated policy issues arise. Most of the issues hinge upon the tradeoff between the free flow of information and the protection of intellectual property and consumer privacy. In section 3 we will discuss these issues and analyze how emerging policies may affect the development of information aggregation. Section 4 concludes our discussion.

## 2. Evolution and Impact of Web Aggregation

The development of web aggregation can have great impact on markets and society. In this section, we will discuss the evolution and analyze the impact of comparison and relationship aggregation.

### 2.1 Comparison Aggregation

Finding the best offers from thousands of e-stores is not an easy task even with the help of a generic search engine. Comparison aggregators, which collect product offering information by crawling e-store sites and organize the collected information for easy retrieval and comparison, have emerged as a helpful intermediary between retailers and consumers. DealTime, mySimon, and bizRate are among the most common comparison aggregators in the U.S. Table 1 compares them with information found at their websites. They have similar features and often have overlap in vendor coverage.

---

<sup>1</sup> Number of Internet hosts in 1999 according to World Bank online data.

Table 1. Comparison of Three Comparison Aggregators

	MySimon	DealTime	bizRate
URL	www.mysimon.com	www.dealtime.com	www.bizrate.com
International Presence	U.S., France, Germany	U.S., U.K.	U.S. only
Scope	1) 2,000 online stores and 32,000 offline services; 2) 250 product categories; 3) 130 paying merchants	1) 4,000 online stores; 2) 26 major categories; 3) 360 paying merchants	1) 1,400 sellers; 2) 19 categories
Listing Requirement	1) Free; 2) Merchants over 3,000 monthly leads are required to pay a fee and receive brand recognition	1) Free; 2) Merchant can pay a fee for brand recognition	1) Free; 2) Merchant can pay a fee for premium placement
Merchant Rating	Gomez	Gomez	bizRate
Personalization	1) Calendar and links to gift searches; 2) Saved searches; Newsletter	1) Shopping advisory; 2) Saved searches; 3) Newsletter	1) Timesaving features (auto form filling, etc.); 2) Exclusive deals; 3) Newsletter
Revenue Model	1) Advertising; 2) Fee based listing; 3) Consulting (search technology)	1) Advertising; 2) Fee based listing; 3) Consulting (search technology)	1) Advertising; 2) Fee based listing; 3) Consulting (market and consumer analysis)

There are many other comparison aggregators in the U.S., e.g., eShop.com (now part of Microsoft’s MSN), PriceGrabber.com, and Clickthebutton.com. Some of the specialized comparison aggregators have been expanding their aggregation categories. For example, PriceScan, an aggregator focused on computer and electronics, has included books, sporting goods, and home & garden into its aggregation offering.

Table 2. Costs and Benefits of Comparison Aggregation

Stakeholders	Benefits	Costs/Risks
Consumers	<ul style="list-style-type: none"> <li>• Convenience and lower search cost</li> <li>• Lower price</li> <li>• Better service</li> </ul>	<ul style="list-style-type: none"> <li>• Possibility to be price discriminated</li> <li>• Minor risk of losing autonomy privacy</li> </ul>
Vendors	<ul style="list-style-type: none"> <li>• Access to vast consumers</li> <li>• Knowledge of competitors</li> <li>• Dynamic pricing</li> </ul>	<ul style="list-style-type: none"> <li>• Increased competition</li> <li>• Less visiting time</li> <li>• Weakening customer relationship</li> <li>• Data could be used by competitors</li> </ul>
Manufacturers	Effective targeted marketing channel	
Aggregators	<ul style="list-style-type: none"> <li>• Establishment as intermediary</li> <li>• Multiple revenue streams</li> </ul>	<ul style="list-style-type: none"> <li>• Profitability</li> <li>• Potential impact of database protection policy</li> </ul>

The impact of comparison aggregation on stakeholders is summarized in Table 2. Comparison aggregation offers many benefits to consumers. It significantly reduces the

search cost in online shopping. This results in increased product variety and lower prices online. In addition, empirical research reveals that not all consumers buy from the vendors that offer the lowest price [2, 3]. The overall service quality, e.g., on time delivery, flexible return policy and friendly customer services, also can significantly affect consumer’s purchasing decisions. Comparison of these characteristics by aggregators results in increased competition beyond price. Consequently, consumers are able to enjoy improved service from online vendors. These benefits, measured in consumer surplus, are estimated to be nearly \$1 billion in book market [4] and over \$6 billion in consumer electronics market [5] in the U.S. Although consumers may have the risk of exposing their consumption pattern to aggregators, this information is often studied collectively without involving any personal data. Consumers may also have a potential risk of being intruded by aggressive targeted marketing campaigns that violate consumers’ autonomy privacy.

Through the service of comparison aggregators, vendors have immediate access to vast potential customers. Small but niche market players can gain consumer awareness through the listing service of aggregators. In addition, comparison aggregation is also a great tool for a vendor to learn its competitors and design competitive offering strategies, e.g., dynamic pricing. For example, Booksamillion.com allows one to compare its price with a number of other online booksellers and dynamically offer a competitive price. Overall, vendors are facing a higher level of competition. Consumers may spend less time visiting their sites, potentially reducing the opportunities of spontaneous selling and weakening the relationship with their customers. The entire databases about various products, part of the valuable assets possessed by the online vendors, are now being freely data-mined by aggregators and can potentially be used by competitors.

Comparison aggregation is also an effective targeted marketing channel. Manufactures and vendors can deliver their messages to customers who are looking for specific products.

Finally, aggregators are becoming more proficient in intermediation by accumulating knowledge about vendors and consumers. They are enjoying multiple revenue streams while expanding their service coverage in terms of product categories and geographical areas. But aggregators are still fairly new entities in the electronic marketplace. They are still experimenting to become a viable business. Critical to their success is their capability of collecting enough vendor data to offer unbiased and relatively complete comparison information. This contingency will be affected if access to vendor data becomes more difficult or costly due to possible future policy changes that advocate online database protection.

## 2.2 Relationship Aggregation

Using “screen scraping” technology, an aggregator can extract account information from different websites on behalf of its customers even without the cooperation of the website owners. Financial institutions initially viewed aggregators as a threat to their operations and tried to block the access by aggregators; First Union National Bank filed a lawsuit in 1999 against PayTrust, an early online bill payment aggregator. Later First Union withdrew litigation and published a set of guidelines for aggregators to follow. By late 2001, over 100 financial institutions, including First Union, and a few web portals are offering account aggregation services. Financial institutions have changed their view to see aggregation as a necessary online banking service and a tool that provides many other benefits, e.g., increased customer loyalty, opportunity for cross selling, and possibility to provide value-added/cost-reducing services such as online bill presentment and payment.

Consumers can also save by eliminating check writing, mailing, and late fees.

### 3. Policy Issues of Web Aggregation

Aggregators collect and reuse information that resides in the public domain or in proprietary systems. Relationship aggregators also deal with vast personal information of individual consumers. Their increasing capabilities and widespread adoption have created concerns about the balance between effective use of information and adequate protection of information providers and consumer privacy. Some unique issues, such as trespassing in cyberspace, have also been brought up in a number of lawsuits against aggregators and require attention because they are not particularly addressed by existing regulations. We will discuss these issues, new policy initiatives, and their implications to the development of information aggregation.

Table 3. Evolution of Relationship Aggregation

	Three Years Ago	Today (2002)	Future
Scope	Single category, e.g., financial or rewards	Multiple categories	A focal point for all personal information needs
Usage	Emergent	1-2 million users	Steadily increasing
Stakeholder Dynamics	1) Aggregators emerged as a new entity with aggregation technology 2) Aggregatees viewed aggregators as a threat	1) Aggregatees see aggregation as a necessity and an opportunity 2) Aggregatees become aggregators 3) Some early aggregators become technology providers	1) Users will include professionals who provide financial planning, management, and advisory services 2) Billers and electronic payment enablers will participate aggregation
Capability	Reporting tool that provides consolidated view and convenience of auto login to other sites	1) Limited fund transfer and bill payment capability 2) Limited availability on mobile devices	1) Full fledged financial management 2) Integration with comparison and other aggregation services 3) Accessible from any network device
Technology	Screen scraping	Screen scraping and limited direct feed using industry standards	Standard based secure information sharing

Table 3 summarizes some of the changes and the trend in relationship aggregation. The capability of fund transfer across organizational boundaries and electronic bill presentment and payment (EBPP) are among the most wanted features of online banking [6]. With the capability of accessing all financial accounts, aggregators are well positioned to provide these services. One of the biggest benefits of these services is cost savings for both billers and consumers. For billers, the transaction cost can be reduced from over \$1 to 2 or 3 cents per bill<sup>2</sup>.

#### 3.1 Database Protection

An aggregator obtains its data from hundreds of thousands of information sources, each containing factual data, such as product prices or daily balances. In legal terms these sources have been called collections of information and databases interchangeably. These databases often take substantial efforts to create and maintain. Therefore database owners have great incentives in protecting their investment.

There are several possible legal mechanisms for conventional database protection, such as trade secrets, contract law, and copyright [7, 8]. But on the Internet, many databases are made available to the general public for free access, eliminating the possibility of trade secret protection. Although some database owners have managed to negotiate licensing agreements with their users, it is costly and sometimes impossible to enforce those contracts.

As to copyright protection, the U.S. Copyright Act of 1976 and its subsequent amendments are to protect “original works of authorship”. Databases, a form of compilation or derivative works of non-copyrightable facts, are only protected to the extent of the creative selection and arrangement of the data. Therefore, in the current copyright protection framework, it is the “originality”, not the effort, that is protected. This principle has been clearly demonstrated in the landmark Supreme Court ruling of *Feist Publications vs. Rural Telephone Co.* in 1991. Feist, a phone directory publisher, copied Rural’s white page listings that had fewer than 8,000 records organized alphabetically by last name. The district court applied the “sweat of the brow” doctrine and granted Rural summary judgment to reward its effort in compiling the listings. But the Supreme Court rejected the doctrine on the basis of the originality requirement of copyright. Rural’s white pages do not

<sup>2</sup> From information presented at the American Bankers’ 2<sup>nd</sup> Annual Account Aggregation Conference, April 23-24, 2001, Virginia, U.S.A.

show any originality because the selection and arrangement of the listings are entirely obvious.

In a similar vein, courts rejected copyright infringement claims found in a number of recent cases against aggregators, such as eBay vs. Bidder's Edge, Ticketmaster vs. Tickets.com, and mySimon vs. Priceman. In fact, aggregators often organize the extracted information and express it in their own ways, predefined or configured by end users. Copyright infringement can hardly stand under this circumstance.

The Internet has allowed access, duplication, and distribution of databases with little cost. Database creators argue that without any effective protection their incentives of creating and maintaining those databases will diminish because of unfair competition from free riders. The European Union first embraced the "sweat of the brow" doctrine and introduced Database Directive in 1996, mandating member nations to implement it by 1998. This directive recognizes the need for protecting the investment of database owners by granting them a *sui generis* (Greek word meaning "of its own kind") right. In the U.K. implementation of the Directive, the Copyright and Rights in Databases Regulations 1997, this special right is called "database right" and is defined as a "property right ... in a database if there has been a substantial investment in obtaining, verifying or presenting the contents of the database". A recent case settled according to this regulation is British Horising Board (BHB) vs. William Hill. Betting service provider William Hill published on its own web site the lists of runners for forthcoming races compiled by BHB without its consent. On February 9, 2001, the High Court of the U.K. ruled that William Hill violated BHB's database right on the accounts that BHB had invested significant amount of time and money in compiling, verifying, and presenting the data and the portions reported by William Hill were substantial with regard to the importance, not the amount, of the information to those interested in horse racing<sup>3</sup>.

Although the "sweat of the brow" theory has been adopted throughout the E.U., it has not been successful in the U.S. Four bills have been introduced since 1996 in the U.S. and all failed to pass. Pressed by the reciprocity provision in the E.U. Database Directive, U.S. attempted a similar bill in 1996 (HR 3531, Moorhead). After its failure, HR 2652 was introduced by Coble in 1997, which received strong opposition from a loose coalition of science groups, libraries, and the industries in telecom, ISPs, and valued-added database producers [7]. Following the enactment of the E.U. Database Directive in 1998, two more controversial bills, HR 354 by Coble and HR 1858 by Bliley, were introduced in 1999 and no agreement was reached by the end of the last session of

the Congress. Internationally, the World Intellectual Property Organization (WIPO) has been considering an international treaty for database protection. As an initial supporter of such a treaty, U.S. quickly changed to an opposing position soon after the withdrawal of HR 3531 in 1996 [7]. It will take tremendous debate and negotiations to form an acceptable framework for database protection worldwide. The major issue is to arrive at an appropriate scope of protection without the risk of creating information monopolies and discouraging downstream innovations based on existing information.

We speculate that the final legislation will have little impact on information aggregation because in most cases the "sweat of the brow" doctrine does not and should not apply to the underlying data extracted by web aggregators. Product databases compiled by online vendors are to inform buyers and facilitate sales of products, not the data. The compilation effort should be accounted as part of product selling activities. The reuse of this data by aggregators is also to inform buyers and facilitate sales of products, which would enhance rather than corrode the initial investment of data compilation. For financial account aggregation, some of the data is the result of user-initiated transactions (e.g., deposit, withdrawal, and fund transfer), which is effectively entered by the user, not the financial institution. In addition, aggregation is performed with authorization from the user who arguably owns the information about himself. The function of the database is very much like a security box in a bank (i.e., users put their personal information in a secure system), accessible by an authorized entity on user's behalf. In both cases the effort of compiling databases does not constitute the core business of aggregatees. This is fundamentally different from the BHB case, where the data is the business.

Even if some of the aggregated data falls under the "sweat of the brow" doctrine, we speculate that the impact of the final legislation on information aggregation will be limited for the following reasons. First, E.U. Database Directive has been regarded as the strictest regulation for database protection. Even so, aggregators have been successfully operating in most E.U. countries, e.g., Klko, PriceRunner, DealTime, mySimon, and CitiBank's account aggregator. Second, factual information, once aggregated, is hard to identify where it originally comes from. Given the large quantity of factual information and huge number of sources involved in aggregation, enforcement is a big problem. Third, as we have seen from preceding discussions, database creators such as small online vendors often gain incredible reach to potential customers through aggregators. The interweaving interests in sharing and reusing information reduce, if not completely eliminate, the need for litigation. Fourth, even database creators need to rely on other sources to compile their databases. In this sense, there are few "pure" database creators. For instance, a vendor compiles its product database using information from

---

<sup>3</sup> News release of BHB on February 9, 2001. Full text can be found at [www.bhb.co.uk/press\\_release.asp?id=255](http://www.bhb.co.uk/press_release.asp?id=255).

manufacturers. And finally, consumers and providers want and need web aggregation evidenced by the compelling benefits discussed earlier. These public interests should not be overlooked and regulations should put structure that guides the exploitation of the new opportunities of web aggregation.

### *3.2 Trespassing in Cyberspace*

Database owners have used another controversial theory, “trespass to chattels”, to charge against online information aggregation activities. For example, eBay claimed that 80,000 to 100,000 daily requests from Bidder’s Edge constituted 1.53% total requests processed by eBay web servers. The court issued a preliminary injunction to stop Bidder’s Edge from aggregating information from eBay based on the reasoning that significant harm could be caused if such activities are allowed. However, in a similar case the court rejected Ticketmaster’s trespass claim against Tickets.com because “it is hard to see how entering a publicly available web site could be called a trespass, since all are invited to enter”<sup>4</sup>.

Legal experts have strongly opposed the application of trespass theory to the Internet. In a friend-of-the-court brief regarding the eBay vs. Bidder’s Edge case, 28 law professors pointed out that it is inappropriate to substitute possible future harm for the actual harm required by the law of trespass to chattels. They concluded that he ruling threatens efficient information exchange on the Internet and the public interests demand a reversal in this case [9]. The case was settled outside of court in early 2001.

Application of trespass theory to other areas of the Internet environment, such as unwanted email, has received similar oppositions because of its pernicious effects to the integrity of the global Internet system [10].

The trespass theory will probably not be accepted within the Internet context. Information aggregation should not trigger this as long as it does not abuse the Internet system (e.g., sending repeated unnecessary requests to cause a denial of service to web servers).

### *3.3 Consumer Privacy Protection*

Easy access to information on the Internet has concerned people about their online privacy. In the U.S., almost two-thirds (63.6%) of Internet users and more than three-quarter (76.1%) of non-users believe that people what go online put their privacy at risk [11]. When it comes to financial data, almost all (94%) consumers are concerned about privacy and security [6]. For financial account

---

<sup>4</sup> This was decided on May 24, 2000. Dramatically, after seeing the decision on eBay case on May 24, 2000, the court later reworked its argument to recognize the potential validity of trespass claim but remained its initial decision of no injunction because of too little evidence of harm. See details at [www.gigalaw.com/library/ticketmaster-tickets-2000-03-27.html](http://www.gigalaw.com/library/ticketmaster-tickets-2000-03-27.html).

related relationship aggregation, privacy and security concerns are the major barriers that prevent people from putting trust in the service. These issues have to be addressed with technical and regulatory measures to fully take advantage of information aggregation.

Privacy protection is very complex in the U.S. There are many privacy related regulations, each having its own context and addressing specific issues. For financial related privacy protection there are Right to Financial Privacy Act, Fair Credit Reporting Act, Federal Educational Rights and Privacy Act, and the most recent Title V of the Financial Services Modernization Act (also known as Gram-Leach-Bliley Act, or GLBA). In addition to its diverse characteristics, U.S. privacy law is also highly decentralized (having both Federal and sometimes divergent State laws) and dynamically evolving [12]. Since no privacy law in the U.S. is specifically designed with the Internet in mind, it is a delicate issue in today’s network environment. Recognizing the complexity, delicacy, and importance of privacy protection, over 100 U.S. corporations, such as IBM, American Express, and AT&T, have appointed their Chief Privacy Officers (CPOs) since 1998 to oversee privacy issues<sup>5</sup>.

The GLBA is one of the recent regulations that are most closely related to information aggregation, especially financial account aggregation. Title V of the Act is dedicated to financial privacy protection, demanding all financial institutions to inform their customers about their handling of nonpublic personal information at least once a year, and give their customers the opportunity to opt-out information sharing with nonaffiliated third parties. For privacy protection purposes, the Act and its corresponding implementations define “financial institution” very widely to cover any company that is engaged in financial activities. For example, a financial software company is considered to be a “financial institution” for privacy protection purposes and if the company sells products or services to consumers, it has obligations to disclose its privacy practices and offer opt-out choices. Clearly, financial account aggregators are “financial institutions”, subject to the privacy provisions in GLBA. With this broad scope, many agencies are involved in the implementation and enforcement of the Act, these include the Office of the Comptroller of the Currency (OCC), The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the Secretary of the Treasury, the National Credit Union Administration (NCUA), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC). These agencies are charged to consult one another to ensure consistencies of the guidelines across all jurisdictions. Aggregators who are technology companies, such as Yodlee, fall under the jurisdiction of

---

<sup>5</sup> “The Rise of the Chief Privacy Officer” by Pamela Mendels, BusinessWeek Online, December 14, 2000.

the FTC, which conducts enforcement by reacting to complaints and does not run routine compliance examinations as banking regulatory agencies normally do. However, these companies will be strictly scrutinized under vendor management guidelines for traditional financial institutions.

The reuse/redisclosure limits in the GLBA regulations provide that an aggregator may only use the aggregated information or disclose it to third parties necessary to perform aggregation service [13]. This may pose a limitation for possible cross-selling opportunities using the aggregate information. On the other hand, if a consumer fails to opt out of information sharing, an aggregator may be allowed to share aggregated information. Between the limitations and opt-out choices, the regulations do not clearly state the legality of either one, leaving the delicate issue to aggregators' own discretion. In order to avoid possible damages to reputation and loss of trust, even in the case where a customer does not opt out for information disclosure, an aggregator should be very careful not to intrude consumer privacy.

Like database protection, privacy protection has its costs and benefits. Without sufficient privacy protection, users will be reluctant to put their privacy at risk and sign up for aggregation services. On the other hand, over protection will significantly increase administrative costs and result in high prices for financial products. For example, implementation of Privacy Directive will cost EU member states \$15-20 billion [14]; U.S. will incur \$9-36 billion implementation cost to avoid "data embargo" of EU [15]. Section 507 of the GLBA allows states to offer greater privacy protection, which could take the form of an "opt-in" approach where consumers have full control of their personal records. This is the exact approach taken by the E.U. in its Privacy Directive. By today's U.S. standard, "opt-in" is too strict and it is strongly opposed by the industries, especially the financial services industry. The Financial Services Roundtable [16] surveyed 90 large banks, insurance and securities companies to estimate consumer benefits from information sharing among institutions. They estimate that the consumers of the 90 institutions can save \$17 billion and 320 million hours per year. The sources of benefits of information sharing include money saved through outsourcing to third parties, relationship pricing and proactive offers; and time saved through call centers, Internet based services, third party services, proactive offers and pre-filled applications.

Similar to database protection, differences of privacy laws between the U.S. and the E.U. have been causing some problems. The E.U. will cut off data flow to the U.S. because they deem that the privacy protection in the U.S. does not meet the minimum requirement of the E.U. Privacy Directive. Some of the differences can be reconciled through the Safe Harbor Agreement negotiated

by the Department of Commerce<sup>6</sup>. Unfortunately, financial services are excluded from the agreement because they are not regulated by the Department of Commerce<sup>7</sup>. In April 2001, the E.U. rejected a U.S. request for postponing the approval of a model contract that financial institutions are asked to sign before sending data to non-E.U. countries. Without resolving this difference, it is impossible for a U.S. aggregator to obtain financial data of their E.U. customers. Even transfer of E.U. employee information to the U.S. for large U.S. based large financial internationals will be difficult.

Policies for privacy protection on the Internet are still at an early stage. The E.U. Privacy Directive has been scheduled for review by collecting experiences of member countries. Required by the GLBA, similar studies in the U.S. will be done by early 2002. These experiences will be helpful for us to understand the issues at hand and hopefully to arrive at appropriate level of privacy protection that can harmonize international differences.

#### 4. Conclusions

Web aggregation is becoming a valuable service for increasingly more Internet users worldwide. It collects existing data on the web and turns them into useful information that lowers search costs and simplifies online relationship management. Meanwhile, it introduces some new risks to consumers, services providers, and other stakeholders. As with any new IT capability, aggregation will be leveraged to minimize risks and bring more value to the society.

Aggregation services are also raising a number of policy issues, primarily concerning the protection of databases and consumer privacy. Both U.S. and E.U. have reacted to address these issues by instituting new policies such as GLBA privacy provisions and E.U. directives for database and privacy. Differences among stakeholders still exist both domestically and internationally. Although it may take a while to reconcile the differences and harmonize the discrepancies, consensus is being built toward an agreement of sufficient protection without jeopardizing the integrity of the Internet. Aggregation will continue to thrive while we are achieving a harmonized policy regime for the information age.

#### Acknowledgement

The study has been supported, in part, by BSCH, Fleet Bank, Merrill Lynch, MITRE Corporation, Singapore-MIT Alliances, and Suruga Bank.

---

<sup>6</sup> See details at [www.export.gov/safeharbor](http://www.export.gov/safeharbor). As of July 26, 2001, there are 78 companies, who claim to meet all the privacy requirements, are on the Safe Harbor List.

<sup>7</sup> From ZDNet UK news, "EU Rejects US Opposition to Privacy Directive", 5/8/2001, by Wendy McAuliffe.

## References

- [1] S.E. Madnick, M.D. Siegel, Seizing the Opportunity: Exploiting Web Aggregation, *MISQ Executive*, 1(1), 2002, 1-12.
- [2] J.P. Bailey, *Intermediation and Electronic Markets: Aggregation and Pricing in Internet Commerce*, Ph.D. dissertation, MIT, 1998.
- [3] M.D. Smith, E. Brynjolfsson, E., Consumer Decision-making at an Internet Shopbot: Brand Still Matters, *Journal of Industrial Economics*, 49(4), 2001, 541-558.
- [4] E. Brynjolfsson, M.D. Smith, Y. Hu, Consumer Surplus in the Digital Economy: Estimating the Value of Increased Product Variety, *WISE 2001*, New Orleans.
- [5] H. Zhu, *A Technology and Policy Analysis for Global E-Business*, MIT Master's Thesis, 2002.
- [6] Star Systems, Inc., Web Aggregation: A Snapshot, August 2002.
- [7] A. Linn, History of Database Protection: Legal Issues of Concern to the Scientific Community, [www.codata.org/codata/data-access/linn.html](http://www.codata.org/codata/data-access/linn.html), 2000.
- [8] J. Askanazi, G. Caplan, K. Donohue, D. Glasser, A. Johnson, E. Mena, E., The Future of Database Protection in U.S. Copyright Law, *Duke Law and Technology Review 0017*, 2001.
- [9] M.A. Lemley, *et al.*, Brief of Amici Curiae in Support of Bidder's Edge, Inc., Appellant, Supporting Reversal, May 24, 2000.
- [10] D.L. Burk, The Trouble with Trespass, *Journal of Small and Emerging Business Law*, 4(1), 2000.
- [11] UCLA, The UCLA Internet Report: Surveying the Digital Future, UCLA Center for Communication Policy, 2000.
- [12] D. Glancy, At the Intersection of Visible and Invisible Worlds: United States Privacy law and the Internet, 16 *Santa Clara Computer and High Technology Law Journal* 357, 2000.
- [13] J.L. Williams, The Impact of Aggregation on the Financial Services Industry, *American Banker's 2<sup>nd</sup> Account Aggregation Conference*, Tysons Corner, Virginia, April 23, 2001.
- [14] S. Davies, Europe to U.S.: No Privacy, No Trade, *Wired.com*, May, 1998.
- [15] R.W. Hahn, An Assessment of the Costs of Proposed Online Privacy Legislation, 2001, available at <http://www.actonline.org/pubs/HahnStudy.pdf>.
- [16] The Financial Services Roundtable, Customer Benefits form Current Information Sharing by Financial Services Companies, December 2000.