The Complexity Underlying JetBlue's Privacy Policy Violations

Annie I. Antón[1], Qingfeng He[1], David L. Baumer[2]

The Privacy Place
North Carolina State University
Raleigh, NC 27695-8207, USA
[1]{aianton,qhe2}@eos.ncsu.edu [2]David_Baumer@ncsu.edu

Abstract

This report examines the actions of JetBlue Airways Corporation (JetBlue), which violated its privacy policy when it gave the travel records of five million customers to Torch Concepts, a private Department of Defense contractor. JetBlue's actions have prompted at least two lawsuits, including a claim by the Electronic Privacy Information Center with the Federal Trade Commission that JetBlue engaged in deceptive trade practices when it violated its privacy policy. Our analysis reveals that JetBlue's privacy policy contains ambiguities, which may pose additional significant threats to customer privacy. The complexity of our actor/information flow model elucidates the importance of organizations establishing clear contractual relationships that specify permissions, obligations and responsibilities for all parties. An implication of this study is that the anti-terrorism exercise of the new Department of Homeland Security described below has taken place at the expense of personal privacy.

1 Introduction

On September 19, 2003, JetBlue Airways publicly acknowledged it had provided the travel records of five million JetBlue customers to Torch Concepts [1, 2, 3, 4], a private DoD (Department of Defense) contractor for an antiterrorism study to track high-risk passengers or suspected terrorists [5, 6]. Torch Concepts then purchased additional customer demographic information (including social security numbers, etc.) about these passengers from Axciom, one of the largest data aggregation companies in the U.S. [4, 7]. The information from JetBlue and Axciom was then used by Torch Concepts to develop passenger profiles for the purpose of identifying possible terrorist suspects [2]. This transfer of data not only directly violated JetBlue's privacy policy [8], it may have also violated Federal privacy laws.[1] In part prompted by a legal complaint from EPIC (Electronic Privacy Information Center), the FTC (Federal Trade Commission) and the DHS (Department of Homeland Security) are currently investigating JetBlue Airways [9] and a private class action suit has been filed in the Utah state courts, which alleges fraudulent misrepresentation and invasions of privacy on behalf of the plaintiffs[2].

Although a complete articulation of the facts has not occurred, the main facts are not in dispute. Our work is based upon information obtained from various public WWW sites, coupled with reports posted on the network that we assume are accurate. The following analysis is derived from our analysis of these materials and press reports.

The remainder of this paper is structured as follows. Section 2 examines the contents of a Torch Concepts report that details how the information obtained from JetBlue was aggregated with information purchased from Axciom. Section 3 models the relationships and information exchanges among the parties

[1] See (http://wwwcdt.org/publications/pp_9.20.shtml) in which Senators Lieberman, Collins, and Levin call on Secretary Rumsfield to investigate whether the Privacy Act of 1974 was violated by the Army because members of the public were not informed, as is required under the Act, that data about them had been collected by a federal agency. See the Privacy Act of 1974, 5 U.S.C. § 552a et seq.

[2] *Halverson et al., v. JetBlue Airways Corporation*, _____Third Judicial District Court, State of Utah. At this stage in the litigation, the plaintiffs are seeking the court's approval to certify them as a class.

involved in the JetBlue case. Section 4 provides an analysis of the JetBlue privacy policy. Finally, Section 5 summarizes our findings.

2 The Torch Concepts Homeland Security Report

Torch Concepts is a defense contractor. According to its web site, Torch Concepts, "are leaders in advanced technology for content management and information mining." Torch, a company with no posted online privacy policy, was the recipient of millions of customer records from JetBlue Airways. The JetBlue privacy policy claims that JetBlue does not transfer customer financial and personal data collected at its web site to third parties. Nevertheless, JetBlue did transfer customer data to Torch Concepts. According to David Neeleman, JetBlue's CEO, "JetBlue provided certain customer data to Torch Concepts, a contractor for the Department of Defense, for a project concerning military base security" [6]. In turn, Torch displayed an inexplicable disregard for the personally identifiable information of the individuals in the JetBlue passenger travel records as evidenced by their posting of a document entitled, "Homeland Security - Airline Passenger Risk Assessment," on the Internet [2]. The Torch Concepts document contained the SSN (Social Security Number) and DOB (Date of Birth) of a specific passenger. At a time when the incidence of identity theft is soaring according to the FTC, nonconsensual displays of SSNs and DoBs are reckless and reprehensible. Torch Concepts removed the report from the Internet on September 17, 2003, but by that time, it had already been reposted on several mirror websites [1, 2, 10]. The transfer of customer data was in response to a special request by the DoD, but in light of unfavorable press coverage, JetBlue has withdrawn from the project [5].

The Torch Concepts Homeland Security document explains that the JetBlue passenger information database was matched with information purchased from Axciom to determine gender, home specifics (renter/owner), years at residence, economic status (income), number of children, SSN, number of adults, occupation, vehicles owned, etc. for 40% of the passengers in the JetBlue database [2]. Torch Concepts was able to leverage the information provided by JetBlue (which they claimed to be limited) into a much larger corpus of information by purchasing demographic information from Axciom to augment the JetBlue passenger information database.

Using this augmented database from JetBlue and Axciom, Torch Concepts found a pattern of anomalous customer records that they believe exists because of erroneous entry, fraud or mischief [2]. Although this may be true, it may also be the case that they have misidentified otherwise law-abiding citizens — a problem that many suspect will also plague the CAPPS II (Computer Assisted Passenger Prescreening System) [11]. CAPPS II is the next-generation passenger screening system administered by the Transportation Security Administration (TSA), a unit of the DHS. The proposed CAPPS II system has been controversial because it would allow the government exceptional power to run background checks on Americans who fly, without providing traditional due process protection in the form of requiring the government to demonstrate individualized probable cause before searching the backgrounds of those who are suspected terrorists [1]. Similar privacy concerns surfaced when the Federal Bureau of Investigation (FBI) launched Carnivore, a software program capable of monitoring millions of email messages from an ISP. The concerns raised about Carnivore, that it enabled the FBI to monitor millions of private email messages without a showing of probable cause, are the same concerns raised by the JetBlue exercise[3].

3 Modeling the Relationships and Information Flows Among the Involved Parties

The JetBlue case is more complex than many previously publicized privacy breaches because of the large number of parties (actors) involved[4]. We modeled this complexity by focusing on the actors, the actual information obtained and used by each of these actors, and whether or not each actor publishes its privacy policy on its website. This model, shown in Figure 1, portrays the apparent contractual relationships in this information transfer and privacy policy violation case. By modeling the various actor

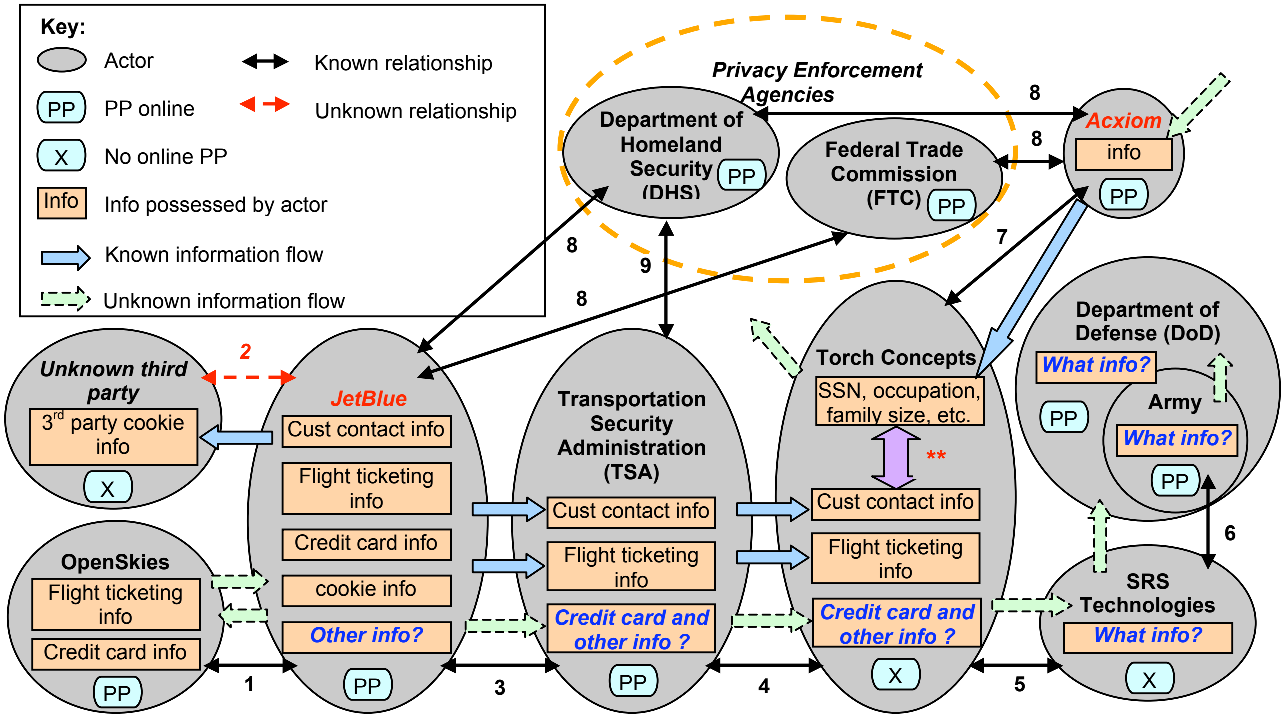
[3] For discussion of how the FBI Carnivore software sniffs email packages see: http://www.fbi.gov/congress/congress00/kerr072400.htm.

[4] In the action the FTC took against Geocities (a subsidiary of Yahoo!) case, Geocities admitted that it violated the terms of its privacy policy, but no other defendants were joined in the suit. See *Geocities*, FTC Dkt. No. C-3849 (Feb. 12, 1999).

dependencies and information flows, we are able to reveal vulnerabilities that, in the case of JetBlue, resulted in unfortunate privacy breaches and two lawsuits.

Figure 1 portrays the relationships among the many actors that in some way handled the sensitive customer information that was first collected by JetBlue and later aggregated by Torch Concepts with additional information from Axciom. The model allows one to develop a better understanding of the internal and external data flows in the JetBlue case. We now discuss these actor relationships and information flows in more detail. According to the JetBlue privacy policy, its ticketing functionality is powered by OpenSkies, but the exact information that is shared by these two parties is still unknown. At a minimum, one must assume that OpenSkies in some way handles the flight ticketing information and financial information of JetBlue customers.

Figure 1: The Actor Relationship and Information Flow Model of the JetBlue Case (Sept. 2003)



1: JetBlue's ticketing functionality is powered by OpenSkies

2: Unknown relationship between JetBlue and an unknown 3rd party

3: JetBlue released partial or full customer info to TSA

4: TSA then turned this info over to Torch Concepts

5: Torch Concepts is an SRS Technologies subcontractor

6: SRS Technologies is a U.S. Army subcontractor

7: Torch Concepts purchased some customer info from Acxiom

8: The FTC and DHS are investigating JetBlue and Acxiom

9: TSA is a unit of the DHS

**: Datamining connected Jetblue cust info and info from Acxiom

After apparent breaches of promises made in its privacy policy were disclosed by the press, JetBlue issued a press release [5] that claims they only released customer contact and flight information to Torch Concepts, but not financial or personal data. Other sources [1], however, including the Torch Concepts report [2], reveal JetBlue actually turned over the complete travel records of 5 million passenger records. The same claims are made by the plaintiffs in two lawsuits that were inspired by apparent breaches of the JetBlue privacy policy. Although JetBlue claimed that "no identifiable customer data was released to any third party, including the Department of Defense or the Transportation Security Administration (TSA)" [5], other sources report that JetBlue first gave the records to the TSA which in turn gave the data to Torch Concepts [1]. In Figure 1, we model this relationship assuming the information in [1] is accurate[5].

As discussed in Section 2, Torch Concepts purchased additional information about the JetBlue passengers from Axciom for use in testing its data-mining theories [1]. Specifically, JetBlue passenger travel records from 2001 and 2002 were matched with data obtained from Axciom to determine passengers' SSN, DOB, occupation, family size, etc. These profiles were then used to flag potential terrorists. The authors are uncertain about how or from where Axciom collected so much sensitive information about consumers. This is denoted using a dotted arrow to Acxiom in Figure 1.

Even though questions remain about further dissemination of this information by Torch Concepts to other organizations including SRS Technologies, the U.S. Army and the Department of Defense, we do know that Torch Concepts further jeopardized the privacy of customer information when its CEO presented the data-mining results at a conference organized by the Tennessee Valley chapter of the national Defense Industries Association on February 25, 2003 [1]. The presentation, which was available on the Internet for over six months, contained a slide with a specific customer's SSN, DOB, name, address, etc. [2]. Given the unknown number of actors to which this information was leaked, it is denoted with an outgoing dotted arrow from Torch Concepts in Figure 1. As previously mentioned, this document is now being reposted on several mirror websites [1, 2, 10]. On some mirror websites, the offending slide was blacked out to protect victims' identities, but on other websites, customers' personal information is still available for free download. We sent email to these websites requesting that they black out the slide containing sensitive information before we published this report.

An organization's on-line privacy policy, when present, can be viewed as that organization's most complete articulation of its privacy policy, especially if no real distinction is made between online and in-person transactions or sales. In fact, some airlines charge less for tickets purchased online. Similarly, just because an organization does not have a privacy policy posted online does not mean that they do not have one at all. However, if such an organization is engaged in business with the public, the absence of a privacy policy means that there is no certainty about the content of their policy and that policy could be changed arbitrarily and without notice. As shown in Figure 1, Torch Concepts, to whom JetBlue's customer travel records were entrusted, does not have an online privacy policy. Moreover, neither does SRS Technologies, which was also granted access to JetBlue customer data. Transmitting sensitive customer data to companies that do not have available privacy policies suggests that JetBlue (or the U.S. Army as the contractor of this effort) was reckless in creating contractual relationships with these organizations before first examining their privacy practices and policies to ensure that customer records would be treated consistently with JetBlue's privacy policies[6].

4 Using Goal-Driven Analysis to Identify JetBlue Policy Violations and Vulnerabilities

To develop a better understanding of JetBlue's privacy practices, we employed a content analysis technique, goal-mining (the extraction of goals from text artifacts) [12], to analyze JetBlue's online privacy policy. Decomposing policy statements into goals makes it easier to establish an objective understanding of an organization's privacy practices and policies. The extracted goals are expressed in structured natural language. These goals were documented in a web-based Privacy Goal Management Tool (PGMT) developed at North Carolina State University (NCSU) [13]. The transformation of privacy practices into structured goal statements condenses the typically long and legalese-laden statements into an objective unit — goals — that can be easily compared to other policies. To identify goals, each statement in the JetBlue privacy policy was analyzed by asking, *"What goal(s) does this statement or fragment exemplify?"* and/or *"What goal(s) does this statement obstruct or thwart?"* All action words are possible candidates for goals. Goals in privacy policies are thus also identified by looking for useful keywords (verbs). The identified goals are worded to express a state that is true, or the condition that holds true, when the goal is realized.

[5] Note further that the same allegations of inappropriate data sharing and revelation are made in the two lawsuits discussed above by EPIC and class action suit in Utah.

[6] Note that JetBlue could have provided some legal protection for itself by stating, in its privacy policy, that "This site contains links to other sites. JetBlue.com is not responsible for the privacy practices or the content of such Websites."

For example the goals G_{328}: DISCLAIM resp[onsibility] *for privacy and security at other sites that we may link to* and G_{1173}: AVOID *sharing CI collected on this site with any 3rd parties* were both extracted from the JetBlue privacy policy. A total of 17 goals were identified from JetBlue's privacy policy and these goals are listed in Table 1.

Table 1: Goals extracted from JetBlue privacy policy (September 2003)

Goal ID	Goal	Actor	Classification
G_{1176}	AVOID collecting offline contact info from children	JetBlue	Protection
G_{20}	AVOID collecting PII from children w/o parental consent	JetBlue	Protection
G_{177}	AVOID distributing [children's] PII w/o prior parental consent	JetBlue	Protection
G_{1179}	AVOID enticing children with game/prize/other activities to divulge more info than needed to participate in necessary booking activity	JetBlue	Protection
G_{1173}	AVOID sharing CI collected on this site with any 3rd parties	JetBlue	Protection
G_{749}	COLLECT CI from our website	JetBlue	Vulnerability
G_{1149}	COLLECT demographic info	JetBlue	Vulnerability
G_{770}	CONTACT cust service for questions about PP	Customer	Unclassified
G_{328}	DISCLAIM resp for privacy and security at other sites that we may link to	JetBlue	Vulnerability
G_{556}	INFORM cust/consumer of org privacy practices	JetBlue	Protection
G_{1178}	PROHIBIT [children] public posting / distribution of contact info w/o prior parental consent	JetBlue	Protection
G_{1174}	PROTECT CI with secure servers	JetBlue	Protection
G_{1172}	USE cookies (optional) to save CI so users only have to enter it once	JetBlue	Vulnerability
G_{1170}	USE IP address to administer institution's website	JetBlue	Vulnerability
G_{1169}	USE IP address to diagnose problems with institution's server	JetBlue	Vulnerability
G_{735}	USE PII to offer products/services	JetBlue	Vulnerability
G_{1175}	USE security measures to protect against loss/misuse/alternation of info under institution's control	JetBlue	Protection

Once goals are identified, they are classified as either privacy **protection goals** or **vulnerabilities**. We have developed a privacy goal taxonomy in which privacy statements are broadly classified as either privacy protection goals or privacy vulnerabilities [12]. *Privacy protection goals* express important consumer privacy rights protections, whereas *privacy vulnerabilities* describe practices that potentially threaten consumer privacy. These two dimensions, privacy protections and privacy vulnerabilities, are extensively intertwined in website privacy policies. To make informed choices, however, it is important to help end-users clearly distinguish between practices that protect one's privacy and practices that introduce potential vulnerabilities. The taxonomy thus provides a framework for understanding relevant privacy issues concerning how institutions treat customer data and the goals make it easier to evaluate an organization's privacy policy within the context of this framework. The fourth column in Table 1 lists the classification for each goal extracted from the JetBlue privacy policy, 41% of which express vulnerabilities to customers' information. Most of the vulnerabilities (5 of 7 goals) concern information collection. The existence of so many vulnerabilities in an organization's privacy policy should itself be of concern to those consumers who are zealous in maintaining their privacy while engaging in the seemingly routine act of ordering a plane ticket online. Unfortunately, it is difficult for customers to discern the extent of privacy vulnerabilities in the privacy policy of JetBlue, which is most probably unintelligible to the average Internet user [13].

Findings

Our analyses enabled us to identify potential vulnerabilities and specific privacy violations by JetBlue as we now discuss.

JetBlue shared personal information with third parties.

JetBlue directly violated its privacy policy that states, "The financial and personal information collected on this site is not shared with any third parties" (G_{1173}). This occurred when passenger travel records were given to Torch Concepts at the request of the DoD. The CEO of JetBlue, David Neeleman, contends that "no payment or credit card information was given by JetBlue", but does admit that personal customer data was transmitted [6].

JetBlue committed a violation of omission by failing to express their use of third party cookies.

JetBlue's privacy policy expressed a cookie related goal: G_{1172} (see Table 1). Cookies are usually set on client machines without the user's awareness if the user does not have protective browser settings. Given that JetBlue's privacy policy does not instruct users how they may set their browser to prompt/block cookies, the "optional" use of cookies is not really optional (see Appendix) because customers are not informed beforehand. Instead, this omission in JetBlue's privacy policy places the burden on users to learn how to set their browser to block cookies, many of whom do not even know what cookies are. Perhaps of greater concern is the fact that JetBlue allows a third party (2o7.net) to set cookies even though there is no mention of third party cookies in the privacy policy. Upon visiting the JetBlue website with our browser set to be prompted before accepting all cookies, we were asked to accept a cookie from 2o7.net. Before accepting this cookie we investigated 2o7.net and were unable to learn anything about this third party or why a cookie was being set by them. If 2o7.net is a third party, as we suspect, this too violates the JetBlue policy simply by its omission of expression in the policy. This is portrayed in Figure 1 as a relationship between JetBlue and an unknown third party.

JetBlue's policy reveals a contractual vulnerability with OpenSkies, Inc.

JetBlue's privacy policy states that they outsource their ticketing support to OpenSkies Inc. However, the privacy policy is unclear about how and what information JetBlue actually shares with OpenSkies. In the previous sentence of its privacy policy, JetBlue explicitly disclaims responsibility for the privacy practices of other websites that JetBlue provides links to. Even though there is no apparent link from the JetBlue website to the OpenSkies website, given the proximity of these privacy statements in the policy, one can only assume that JetBlue thus disclaims responsibility for OpenSkies' privacy practices. Thus, JetBlue is sharing sensitive customer information with no control over how their affiliates are protecting their customers' information. Once again, the burden is placed on the end user to determine if OpenSkies will protect sensitive customer information.

Ambiguities in JetBlue's privacy policy point to potential vulnerabilities, raising a virtual red flag.

The JetBlue privacy policy, states "Our ticketing functionality is powered by OpenSkies Inc. The financial and personal information collected on this site is not shared with any third parties." The careful reader will note that from these two sentences, the subject to which "this site" refers is unclear. If it refers to JetBlue, it is unclear why JetBlue is collecting financial information and how this information is collected given that the ticketing functionality is powered by OpenSkies. If it refers to OpenSkies, JetBlue is claiming the practices of OpenSkies as its own. Finally, this directly contradicts the statement: "JetBlue is not responsible for the privacy practices or the content of such Websites."

The JetBlue privacy policy over-emphasizes COPPA-related issues.

Five of the 17 goals expressed in the JetBlue privacy policy concern collection of information from children. However, JetBlue's online business/practices basically have nothing to do with children. Given this unusual emphasis on COPPA-related (Children's Online Privacy Protection Act) issues, one is left to assume lack of awareness or experience in policy specification on the part of JetBlue's privacy policy author. Ironically, some JetBlue customers' number of children was among the information that Torch Concepts used in its data mining efforts.

5 Conclusions

The preceding analysis was conducted by making use of material found on the Internet. As such, there may be other information that we have not seen that could provide additional details. Our objective was to provide a holistic analysis given the information currently available to the public. Whether the U.S. government should develop passenger prescreening systems, such as CAPPS II, is beyond the scope of this paper. It is not, however, improper to criticize incontinent release of actual customer data in connection with an anti-terrorist training exercise. Additionally, the JetBlue Airways privacy policy violation case is quite complex, involving many actors and resulting in apparently unintended consequences. The impacts of this case are so far reaching that it should be studied by anyone concerned about preserving consumer privacy in connection with efforts of the DHS to identify and thwart terrorists. We conclude our report with several observations and recommendations.

First, as discussed in Section 3, many organizations handled sensitive information in the JetBlue Airways case, two of these organizations do not have an online privacy policy (Torch Concepts and SRS Technologies). This causes one to speculate about whether these organizations are committed to protecting the privacy of those individuals whose information they collect and handle. Virtually all commentators who are concerned about consumer privacy recommend that organizations with a website presence on the Internet should publicly post their privacy practices and policies. Posting a privacy policy online is subtle form of self-regulation and given the willingness of the FTC to sue those who do not adhere to their own privacy policy, it ensures that organizations are accountable for their actions.

Second, organizations must go beyond simply posting an online privacy policy. Care must be taken to ensure that a policy is well-written and accurate. Our evaluation of the JetBlue privacy policy revealed ambiguities, violations, vulnerabilities, over-emphasis of some irrelevant issues (obtaining information from children) while, at the same time, omitting other items of greater importance (see Section 4). Organizations should employ privacy policy specification templates or wizards in conjunction with the techniques discussed in this report (actor/information flow modeling and goal-driven analysis) to avoid the weaknesses exhibited in the JetBlue policy and to ensure compliance with their policies by third parties.

Third, even though a company may have a well-written privacy policy, it does not guarantee consumer privacy protection. JetBlue violated its privacy policy by disclosing customer information to third parties without informing its customers. Although it is challenging for organizations to enforce their privacy policies, the introduction of privacy legislation (COPPA, GLBA and HIPAA) is indicative of a concerted movement to require firms in regulated industries to aggressively comply with the relevant statutory privacy protections. This case suggests a need to consider enactment of comprehensive privacy laws governing all business entities, especially those not subject to GLBA and HIPAA, as well as a need to continue vigorous enforcement by the FTC against firms that violate their own privacy policies.

Fourth, the transfer of customer data from JetBlue to Torch Concepts took place "in response to a special request from the Department of Defense", according the JetBlue CEO, David Neeleman [6]. The lamentable releases of raw customer data by a defense contractor suggests that the DoD did not stress the importance of preserving consumer privacy and the dangers of identity theft as a result thereof to JetBlue. If the government is going to engage in wholesale examinations of consumer data through its proxies, such as Torch Concepts, the relevant government officials should apprise these contractors of the importance of preventing public disclosure of data that could result in harm to these consumers. If government officials conducting these anti-terrorism exercises are unaware of privacy laws and the importance citizens attach to privacy, then the training of government officials should be substantially augmented in the area of privacy and privacy laws.

Fifth, the JetBlue case involved many parties (some which JetBlue may not have been aware of). It seems probable that the existence of so many contractual relationships, marked by widespread transfer of sensitive information, increased the likelihood of privacy vulnerabilities (see Figure 1). Many organizations, especially financial institutions, have established equally complex contractual relationships with subsidiaries, affiliates and business partners. This complexity bewilders consumers, especially when organizations disclaim responsibility for the privacy practices of those organizations with whom they share a contractual relationship. The complexity of the contractual relationships and disclaimers buried in the middle of privacy policies undermine the ability of consumers to make informed privacy choices.

Finally, the JetBlue Airways case exemplifies how desirable it is for organizations to explicitly consider internal and external rights, obligations and permissions to ensure that they operate in accordance with their privacy policies and that their privacy policies are comprehensible to ordinary users or consumers. In this report, we used goal-driven analysis to enable us to develop an understanding of JetBlue's privacy policies as well as to identify potential vulnerabilities. Additionally, we modeled the parties involved in the case in conjunction with the information transactions that transpired leading up to FTC and DHS investigations. Using our model of relational commitments, or lack thereof, among the parties (actors) involved, the privacy faux pas that ocurred, now seems inevitable. A company that has a privacy policy and claims to be concerned about customer privacy cannot credibly transfer large amounts of data to firms that do not have privacy policies and disclaim any responsibility for the actions of other firms who receive such data. In the future, it is hoped that proactive management can forecast privacy breaches and take steps to avert such contingencies [14].

Acknowledgements

The authors wish to thank Gene Spafford for suggesting that we conduct this study and for his comments on drafts of this report. Additional comments were provided by ThePrivacyPlace.Org staff.

References

[1] *JetBlue Privacy Scandal*, DontSpyOnUs, by Bill Scannell, Downloaded on Oct 18, 2003. http://dontspyon.us/jetbluescandal.html

[2] *Homeland Security - Airline Passenger Risk Assessment,* Torch Concepts, February 23, 2003. http://www.computerbytesman.com/privacy/jetblue/

[3] JetBlue 'Fesses Up, Quietly, Wired News, by Ryan Singel, September 19, 2003. http://www.wired.com/news/politics/0,1283,60502,00.html

[4] JetBlue Shared Passenger Data, Wired News, by Ryan Singel, September 18, 2003. http://www.wired.com/news/privacy/0,1848,60489,00.html

[5] *The press release regarding JetBlue's retention of Deloitte & Touche to assist in its analysis of its privacy policy*, September 22, 2003. http://www.jetblue.com/learnmore/pressDetail.asp? newsId=202

[6] *A letter from JetBlue's CEO, David Neeleman, concerning JetBlue's commitment to protecting customer privacy*, September 23, 2003. http://www.jetblue.com/learnmore/privacypolicy.html

[7] *EPIC Submits Privacy Complaint To FTC Regarding JetBlue*, Tech Law Journal, download on October 16, 2003. http://www.techlawjournal.com/topstories/2003/20030922.asp*Army Admits Using JetBlue Data*, Wired News, by Ryan Singel and Noah Shachtman, September 23, 2003. http://www.wired.com/news/conflict/0,2100,60540,00.html

[8] *JetBlue's Online Privacy Policy*, JetBlue Airways, September 24, 2003. http://www.jetblue.com/privacy.html

[9] *JetBlue Target of Inquires by 2 Agencies*, New York Times, by Philip Shenon with John Schwartz, September 23, 2003. http://www.nytimes.com/2003/09/23/business/23PRIV.html?ex=1064894400&en=7276cef7f8f0e23c&ei=5062&partner=GOOGLE

[10] *Homeland Security - Airline Passenger Risk Assessment, American Civil Liberties Union*, downloaded on October 18, 2003. http://www.aclu.org/Privacy/Privacy.cfm?ID=13686&c=40

[11] *Coalition Letter on Passenger Profiling,* Electronic Privacy Information Center, March 25, 2003. http://www.epic.org/privacy/airtravel/capps_letter_032503.html

[12] A.I. Antón and J.B. Earp. A Requirements Taxonomy to Reduce Website Privacy Vulnerabilities, To Appear: *Requirements Engineering Journal*, Springer-Verlag, 2004.

[13] A.I. Antón, J.B. Earp, D. Bolchini, Q. He, C. Jensen and W. Stufflebeam. The Lack of Clarity in Financial Privacy Policies and the Need for Standardization, *NCSU CSC Technical Report TR-2003-14*.

[14] D.L. Baumer, R Iyengar, and R.P. Moffie, Legal Liabilities of Website Operation and Internet Privacy Issues, *Internal Auditing*, Vol. 18(5), Sept.-Oct. 2003, pp: 22-27.

Appendix A — JetBlue's Online Privacy Policy

(Downloaded on September 24, 2003, two days after the FTC and DHS announced JetBlue investigations)

JetBlue Airways has created this privacy statement in order to demonstrate our firm commitment to privacy. The following discloses our information gathering and dissemination practices for this website: JetBlue.com.

We use your IP address to help diagnose problems with our server, and to administer our Web site. We use cookies (optional), to save your name, email etc. so you don't have to re-enter it each time you visit our site.

Our optional site's registration form requires users to give us contact information (like their name and email address) and demographic information (like their zip code). We use customer contact information from the registration form to send the user updates and offers from JetBlue. This site contains links to other sites. JetBlue.com is not responsible for the privacy practices or the content of such Websites.

Our ticketing functionality is powered by OpenSkies Inc. The financial and personal information collected on this site is not shared with any third parties, and is protected by secure servers.

Security

This site has security measures in place to protect against the loss, misuse and alteration of the information under our control.

Children's Guidelines

It is the policy of JetBlue Airways:

1. NOT to seek to collect online contact information from children without prior parental consent or parental notification.

2. NOT to seek to collect personally identifiable offline contact information from children.

3. NOT to distribute to third parties any personally identifiable information with out prior parental consent.

4. NOT to give the ability to publicly post or otherwise distribute personally identifiable contact information without prior parental consent.

5. NOT to entice children with the prospect of a special game, prize or other activity or to divulge more information than is needed to participate in the necessary booking activity.

Contacting the Web Site

If you have any questions about this privacy statement, the practices of this site, or your dealings with this Web site, you can contact us at DearJetBlue.com.