

*Beyond Contract: Utilizing Restitution to Reach Shadow Offenders & Safeguard Information Privacy*

Marcy E. Peek\*

Abstract

The author argues that liability under the theory of restitution should be imposed on third party companies that mishandle an individual's personal data. These third party companies are generally information brokers and aggregators that compile personal information on millions of individuals from a variety of commercial and governmental sources. The author calls such entities "shadow offenders" because they generally have no direct commercial or contractual relationship with consumers and lack privity of contract with consumers. Largely because of this lack of a direct commercial relationship, shadow offenders often escape notice and legal liability for their handling of personal data. A restitutionary remedy for victims of improper data use and handling at the hands of such entities would apply in cases wherein shadow offenders are unjustly enriched by their mishandling or misuse of personal information. Such a remedy would incentivize such third party companies to properly safeguard and handle personal information where, traditionally, few such incentives have existed. In addition, a remedy based in restitution would not only allow for a form of recovery that avoids the problems associated with attempting to bring causes of action based primarily in contract, but would also offer a means of redress that does not depend on conceptualizing personal data as property or calculating the monetary value of data to the individual. Finally, in contrast to public remedies obtained under consumer protection statutes, the restitutionary remedy allows for individualized recovery by consumers whose personal information is mishandled, misused, or improperly safeguarded.

---

\* Assistant Professor of Law, Whittier Law School. I would like to thank the Center for Internet and Society at Stanford Law School ("the Center"), which made this project possible. An earlier version of this paper was presented in March 2004 at a privacy symposium sponsored by the Center.

## Prologue

Recently, the FBI discovered that an employee of a data-marketing firm had hacked into an Acxiom server for more than two years.<sup>1</sup> The data marketing employee “[helped] himself to unencrypted data belonging to 10% of Acxiom’s customer base -- upwards of 200 large companies.”<sup>2</sup> Acxiom, which maintains records on 96% of American households, is the largest aggregator of personal data in the world.<sup>3</sup> It gives its corporate customers what it calls “real-time, 360-degree views”<sup>4</sup> into consumers by assigning individuals a 13-digit code. This code tracks us throughout life, and is used to place us into one of 70 lifestyle clusters, which changes as the information Acxiom holds on us is updated.<sup>5</sup>

After it was reported that the data-marketing firm employee had accessed Acxiom’s server, the FBI discovered that, in an unrelated case which the Department of Justice has described as “the largest cases of intrusion of personal data to date,”<sup>6</sup> employees of a Florida-based Internet advertising company hacked into Acxiom’s server for more than a year, accessing records on millions of Americans.<sup>7</sup>

The year before, records on five million JetBlue Airways (“JetBlue”) passengers<sup>8</sup> were allegedly improperly disclosed and mined<sup>9</sup> by a company called Torch Concepts,

---

<sup>1</sup> See Richard Behar, *Never Heard Of Acxiom? Chances Are It's Heard Of You*, *Fortune*, Feb. 23, 2004, p. 140.

<sup>2</sup> Behar, *supra* note 1. The employee, Daniel Baas, “illegally obtained about 300 passwords, including one that acted like a “master key” and allowed him to download files that belonged to other Acxiom customers.” United States Attorney’s Office for the Southern District of Ohio, *Press Release: Milford Man Pleads Guilty to Hacking*, December 18, 2003, <http://www.usdoj.gov/usao/ohs/Press/12-18-03.htm>.

<sup>3</sup> Acxiom handles over a billion records each day, and does over one billion dollars in annual sales. See Behar, *supra* note 1. Acxiom has detailed and personal information on most Americans such as our social security number, credit card accounts, and buying patterns. See *id.*

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

<sup>5</sup> See *id.* Personal life events “such as marriage, the purchase of a home, the birth of a child or preparation for retirement are likely to result in a cluster change.” *Daily Briefing*, *The Commercial Appeal*, Aug. 4, 2004, C2 (2004 WL 84688060).

<sup>6</sup> United States Department of Justice, *Press Release: Florida Man Charged with Breaking into Acxiom Computer Records*, July 21, 2004, [http://www.usdoj.gov/opa/pr/2004/July/04\\_crm\\_501.htm](http://www.usdoj.gov/opa/pr/2004/July/04_crm_501.htm). One of the hackers was indicted and charged with “139 counts of illegal access, representing approximately 8.2 gigabytes of data which were downloaded from the Acxiom server from approximately April 2002 to August 2003.” *Id.*

<sup>7</sup> See Behar, *supra* note 1.

<sup>8</sup> The information included, at a minimum, name, address telephone and itinerary-related information. *Electronic Privacy Information Center’s Complaint Against JetBlue Airways and Acxiom Corporation to the Federal Trade Commission*, September 22, 2003, <http://www.epic.org/privacy/airtravel/JetBlue/ftccomplaint.html> (“EPIC Complaint”). See also Consolidated Class Action Complaint, *In re JetBlue Privacy Litigation*, 2004 WL 578605 (February 4, 2004).

<sup>9</sup> Data mining “generally refers to techniques for extracting summaries and reports from an organization’s databases and data sets.” The Sedona Conference Working Group on Electronic Document Retention and Production, *The 2004 Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 5 Sedona Conf. J. 151, 201 (2004). More specifically, “[d]ata mining is the enhanced ability to analyze vast amounts of personal information. The data mining tools, also known as Knowledge Discovery in Databases, or KDD applications, search for patterns and clusters within datasets,

allegedly for national defense purposes. The passenger information was disclosed without the passengers' knowledge or consent. In that case, Torch Concepts was the third-party information mining company that obtained the passenger data from JetBlue and controlled many aspects of the project.<sup>10</sup> Torch Concepts also independently, and as part of the same project, purchased additional data on two million JetBlue passengers from Acxiom; the demographic data acquired included a host of sensitive information such as gender, income, number of children, social security number, occupation, and vehicle information.<sup>11</sup> Torch then allegedly used the aggregate data to perform a detailed customer profiling and terrorism risk assessment study, and proceeded to present its findings at an engineering conference, including the social security number and other identifying information of one individual whom it identified as potentially high-risk.<sup>12</sup> Later, Torch proceeded to post its profiling and risk assessment results on a publicly available website.

## I. Information Alienation at the Hands of Shadow Offenders

### Introduction

Our personal data is not our own. Companies are, by and large, free to gather, aggregate, distribute and share<sup>13</sup> our personal information *ad infinitum* and as they see fit.<sup>14</sup> The personal information alienation that we are experiencing on a grand scale<sup>15</sup>

---

without receiving a hypothesis from the analyst and do so in an almost fully automated process.” Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. of Miami L. Rev. 991, 995 (2004).

<sup>10</sup> Torch Concepts received the personal data directly from Acxiom (JetBlue's subcontractor) at JetBlue's request. See EPIC Complaint, *supra* note 8. See also Edward Alden, *Protests Force Curbs on Tools of Suspicionless Surveillance*, Financial Times, October 2, 2003, at 22. Torch Concepts was a subcontractor of SRS Technologies, a California-based company, and it was allegedly “through [the contract with SRS Technologies that] Torch used [the passenger] information to perform a highly detailed passenger profile study.” Consolidated Class Action Complaint, *In re JetBlue Privacy Litigation*, 2004 WL 578605 (February 4, 2004).

<sup>11</sup> Department of Homeland Security Privacy Office, *Report to the Public on Events Surrounding JetBlue Transfer*, February 20, 2004, available at <http://www.cdt.org/privacy/20040220dhsreport.pdf>.

<sup>12</sup> Consolidated Class Action Complaint, *In re JetBlue Privacy Litigation*, 2004 WL 578605 (February 4, 2004).

<sup>13</sup> “Affiliate information sharing,” for example, “represents a growing risk to individuals' privacy. Companies, such as Citibank with its 1,900 affiliates, or Bank of America, which has more than 1,000 entities in its corporate family, can transmit your information for cross-selling or marketing to an unlimited degree under federal law.” Chris Hoofnagle, *Is Your Life an Open Book? And Who's Reading it?*, Sept. 8, 2003, *Akron Beacon Journal*, available at <http://www.ohio.com/mlb/beaconjournal/news/editorial/6706395.htm?1c>.

<sup>14</sup> This wide latitude is subject only to limited exceptions such as medical records, video rental records, student records, and cable television consumer data. The financial services industry is subject to the relatively watered-down Graham-Leach-Bliley Act of 1999, also known as the Financial Services

has engendered a society in which our personal data is by default public and subject to outside scrutiny and disclosure.

A specific example of this alienation of personal information, and the dilemma addressed in this paper, is the problem of data mishandling, misuse and improper safeguarding at the hands of entities that I call “shadow offenders,” third party companies that traffic in personal data yet have no direct commercial or contractual relationship with the individual. This piece argues that in cases of improper use, handling, or safeguarding of personal data by such companies, recovery in restitution should be available for the individual victims.

a. Data Trafficking by Third Party Shadow Offenders

The widespread phenomenon of data handling and mishandling<sup>16</sup> at the hands of shadow offenders offers a paradigmatic portrait of the abuse of personal data. Shadow offenders have access to large amounts of personal data on millions of individuals and are largely unaccountable for their use of that data. They operate virtually outside the

---

Modernization Act. See CALPIRG Education Fund, *Financial Privacy in the States*, 4-5 (2004). See generally CALPIRG, *Privacy Denied: A Survey of Bank Privacy Policies* (August 2002); Federal Trade Commission, *Financial Privacy: The Gramm-Leach Bliley Act*, <http://www.ftc.gov/privacy/glbact/index.html> (last accessed on September 13, 2004). In addition, furnishers of personal credit information are subject to the Fair Credit Reporting Act, 15 U.S.C. 1681, *et seq.*

15

“Over the past few decades, there have been dramatic expansions in the quality, the breadth, and the intensity of programs that use new generations of technology for gathering, storing, sharing and using information . . . If we add up all the frequently overlapping profiles encompassing medical records, academic and professional performance, credit ratings, consumer behavior, insurance records, driving records, law enforcement data, welfare agency information, child support enforcement programs, Internet communications, and other information systems, it is safe to say that much of the significant activity of our lives is now subject to systematic observation and analysis.”

Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* 12 (2000).

<sup>16</sup> See generally Pamela Samuelson, *Privacy as Intellectual Property*, 52 *Stan. L. Rev.* 1125, 1126 (2000) (discussing the collection and processing of personal information in cyberspace).

penumbra of legal liability not only because their access, use, and misuse of personal data goes unrecognized, but also because they are not in a direct commercial relationship or in privity of contract with the consumer. Largely because of this lack of privity,<sup>17</sup> third party entities have little incentive to protect, or even ensure the accuracy of, personal data.

These third-party actors are often information brokers and data miners; prominent examples of such companies are ChoicePoint and Acxiom.<sup>18</sup> Their specialty is the collection, aggregation, and analysis of personal data from a wide range of public and private sources;<sup>19</sup> the information is primarily used for profiling and marketing purposes.<sup>20</sup> ChoicePoint, for example, “owns an astounding 19 billion records, about 65 times as many pieces of information as there are people in the United States. As a result, ChoicePoint knows more about most people than the federal government does.”<sup>21</sup>

---

<sup>17</sup> "The doctrine of privity means that a person cannot acquire rights or be subject to liabilities arising under a contract to which he is not a party." Black's Law Dictionary 1218 (1999) (quoting G.H. Treitel, *The Law of Contract* 538 (8th ed. 1991)).

<sup>18</sup> See generally Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Information for Law Enforcement*, 29 N.C. Journal of International Law and Commercial Regulation 595 (2004); Edmund Mierzwinski, *Data Dealers Seizing Control Over Our Lives*, U.S. PIRG, <http://www.pirg.org/consumer/dsefoped.htm> (last accessed on September 12, 2004).

<sup>19</sup> "By drawing from . . . three sources of information—public records, internal records, and external records—profilers may have a detailed marketing dossier, which includes demographic and psychographic information. A profile available from a national-list compiler could include: name, gender, address, telephone number, age, estimated income, household size and composition, dwelling type, length of residence, car ownership, pet ownership, responsiveness to mail offers, contributor status, credit card ownership, lifestyle, hobbies, interests, and neighborhood characteristics including average education, house value, and racial composition." United States Department of Commerce, *Privacy and the NII: Safeguarding Telecommunications Personal Information*, October 1995, <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>.

<sup>20</sup> The data are culled from a wide variety of sources such as credit card records, motor vehicle records, court databases, magazine subscriptions, survey results, and product warranty cards. "ChoicePoint and other collectors scoop up these pieces of information and preserve them electronically. They buy the data -- sometimes from each other -- or obtain it from public sources, such as court and property records. Then, when their customers ask, ChoicePoint blends the pieces into a picture of you. Where you've lived. The cars you drive. The people you know -- neighbors, school friends, ex-spouses. The more records, the bigger the picture." Shane Harris, *Private Eye*, Government Executive, March 16, 2004, <<http://www.govexec.com/features/0304/0304s1.htm>>.

<sup>21</sup> Harris, *supra* note 20.

The mishandling and cavalier treatment of our personal data at the hands of third-party offenders -- which, in many cases, is likely to remain undiscovered or unreported -- takes many forms, including the unauthorized disclosures of personal information to inappropriate parties, security breaches due to hacking and insider abuse,<sup>22</sup> and the cavalier sharing of information from these third party companies to numerous companies down the line.

Such data errors and instances of data insecurity lead to problems such as consumer fraud and identity theft for millions of individuals.<sup>23</sup> For example, the Federal Trade Commission ("FTC") recently conducted a study that concluded that over 27 million Americans have been victims of identity theft in the last five years -- almost 10 million in the last year alone,<sup>24</sup> identity theft cost individual victims \$5 billion in out-of-pocket expenses in 2003.<sup>25</sup> A recent informal study found that lists of credit card numbers are easily accessible by performing simple search functions in basic search engines such as Google.<sup>26</sup> More broadly, the exposure of personal and sensitive information leaves individuals vulnerable to inappropriate uses of their data by companies utilizing or exposing their information in ways not originally intended or even imagined by the consumer. These problems of data mishandling and data misuse

---

<sup>22</sup> One expert estimates that "on the black market . . . each set of identity information is worth several hundred dollars. A database . . . with thousands or perhaps millions of people's information, then, can garner quite a bundle for the thief." Kimberly Hill, *Acxiom Data Theft Worries Millions of Customers*, CRM Daily, July 24, 2004, [http://crm-daily.newsfactor.com/story.xhtml?story\\_title=Acxiom-Data-theft-Worries-Millions-of-Customers&story\\_id=26009&category=custdata](http://crm-daily.newsfactor.com/story.xhtml?story_title=Acxiom-Data-theft-Worries-Millions-of-Customers&story_id=26009&category=custdata).

<sup>23</sup> See generally CALPIRG Education Fund, *Financial Privacy in the States*, February 6, 2004, available at <http://calpirg.org/CA.asp?id2=12145&id3=CA&>; CALPIRG Privacy Rights Clearinghouse, *Nowhere to Turn: Victims Speak out on Identity Theft* (May 2000), available at <http://www.privacyrights.org/ar/idtheft2000.htm>.

<sup>24</sup> Federal Trade Commission, *Identity Theft Survey Report*, September 2003, <http://www.ftc.gov/os/2003/09/synovatoreport.pdf>.

<sup>25</sup> See *id.*

<sup>26</sup> Pam Baker and Ben Baker, *Google Search Reveals Credit Card Information*, CRM Daily, September 15, 2004, [http://crm-daily.newsfactor.com/story.xhtml?story\\_id=26967](http://crm-daily.newsfactor.com/story.xhtml?story_id=26967).

exemplify the fundamental tension that exists between consumers, who have a pressing interest in protecting their private information, and private companies, which have enormous economic incentives to share and sell that private information,<sup>27</sup> coupled with a lack of legal incentives to properly safeguard such information.

## II. Utilizing Restitution as a Remedy

### a. The Restitutionary Doctrine

In these shadow offender cases of data mishandling and improper usage, principles of restitution should be applied to remedy cases of unjust enrichment to third-party companies that mishandle, misuse or improperly safeguard individuals' data.

Restitution, which is properly understood both as a source of liability and a remedy,<sup>28</sup> looks to the value of a benefit conferred on a defendant by a plaintiff. The restitution cause of action springs from the receipt of a benefit “under circumstances such that its retention without payment would result in the unjust enrichment of the defendant at the expense of the plaintiff.”<sup>29</sup> As a remedy, “the defendant must either restore the

---

<sup>27</sup> For example, in 2003, “the financial services industry pocketed more than \$937 million in California alone from the sale and sharing of consumers’ private information.” CALPIRG Education Fund, *Financial Privacy in the States*, *supra* note 23.

<sup>28</sup> See Tracy A. Thomas, *Justice Scalia Reinvents Restitution*, 36 Loy. L.A. L. Rev. 1063, 1066 (2003) (“[R]estitution as a remedy can be used with a restitution liability theory or with a regular type of contract, tort, or property claim.”); David F. Partlett & Russell Weaver, *Restitution; Ancient Wisdom*, 36 Loy. L.A. L. Rev. 975, 981 (2003) (noting the “misperception that restitution is itself just a remedy.”). See also Black’s Law Dictionary (7<sup>th</sup> ed. 1999) (“[Q]uantum meruit is . . . an equitable remedy to provide restitution for unjust enrichment. It is often pleaded as an alternative claim in a breach-of-contract case so that the plaintiff can recover even if the contract is voided.”)

<sup>29</sup> Restatement (Third) of Restitution and Unjust Enrichment § 1 (Tentative Draft 2004). See also Restatement (First) of Restitution § 1 (1937) (“A person who is unjustly enriched at the expense of another is liable in restitution to the other.”)

benefit in question (or its traceable product), or else pay money in the amount necessary to eliminate unjust enrichment.”<sup>30</sup>

The defendant does not have to act tortiously, wrongfully or in bad faith<sup>31</sup> in its acquisition of a benefit (although in such cases the remedy may be determined by reference to plaintiff’s losses rather than defendant’s benefit)<sup>32</sup> and the remedy of restitution is not punitive.<sup>33</sup> Indeed, “enrichment” merely requires that a person “has received a benefit. A person is unjustly enriched if the retention of the benefit would be unjust.”<sup>34</sup> Not only is the law of restitution not tied to tortious or wrongful behavior, but also there is no requirement that a defendant dispossessed a plaintiff of property, chattels, or money<sup>35</sup> – or even that the plaintiff performed a service for the defendant. Rather, a person is deemed to have conferred a benefit to another under the law of restitution if she “in any way adds to the other’s security or advantage”;<sup>36</sup> “the word ‘benefit,’ therefore, denotes any form of advantage. The advantage for which a person ordinarily must pay is

---

<sup>30</sup> Rest. (Third) of Restitution and Unjust Enrichment § 1 (Tentative Draft 2004). *See also Interform Co. v. Mitchell*, 575 F.2d 1270, 1278 n. 4 (9<sup>th</sup> Cir. 1978) (“in unjust enrichment [cases] . . . the recovery granted is not based upon a contract and . . . the underlying standard for the recovery is the net benefit conferred upon the defendant.”); John D. Calamari & Joseph M. Perillo, *The Law of Contracts* § 9-23, at 376 (3d ed. 1987) (“‘Restitution’ is an ambiguous term, sometimes referring to the disgorging of something which has been taken and at times referring to compensation for injury done.”)

<sup>31</sup> *See, e.g., Werlin v. Reader’s Digest Ass’n, Inc.*, 528 F.Supp. 451, 466 (S.D.N.Y. 1981) (defendant held liable under theory of unjust enrichment where it benefited at the expense of plaintiff yet “did not act in bad faith.”) The drafters of the proposed Restatement (Second) of Restitution explained that the law of restitution is based both on “wrongful acquisition of a gain” and on “harm or loss wrongfully imposed.” Restatement (Second) of Restitution, Introductory Note (Tentative Draft No. 1 1983). More specifically, “[i]n some cases the fact a person has acquired a gain by wrongdoing is the principal reason for requiring him to make restitution. . . In other cases no element of wrongdoing is present.” *Id.*

<sup>32</sup> *See infra*, Part II, section d (“Calculating Recovery”).

<sup>33</sup> Restatement (First) of Restitution I, 8, 2 Intro. Note (1937). *See also 3Com Corp. v. Electronics Recovery Specialists, Inc.*, 104 F. Supp.2d 932 (N.D. Ill. 2000) (punitive damages not recoverable in restitution cases); Andrew Kull, *Restitution’s Outlaws*, 78 Chi.-Kent L. Rev. 17, 17 (2003).

<sup>34</sup> Restatement (First) of Restitution § 1, cmt. a (1937).

<sup>35</sup> *Cf. Werlin, supra* note 31, at 465 (in certain intellectual property cases, “the courts have held that, even if the plaintiff has no property right in an idea, and even though no express or implied-in-fact contract for the sale or use of such an idea has been established, the defendant may, in appropriate circumstances, nevertheless be found liable to the plaintiff in quasi-contract on a theory of unjust enrichment.”).

<sup>36</sup> *Ohwell v. Nye & Nissen Co.*, 26 Wash.2d 282, 285, 173 P.2d 652, 653 (1946) (quoting Restatement (First) of Restitution § 1 (1937)).

pecuniary advantage; it is not, however, necessarily so limited.”<sup>37</sup> Furthermore, no contractual relationship need exist for a restitutionary cause of action to arise; in fact, while contract law recognizes a remedy of restitution for breaches of contracts<sup>38</sup> and other situations peculiar to contractual situations (such as impossibility), the restitution cause of action is a quasi-contractual remedy; in other words, it is implied by law.

Modern restitutionary scholars have identified one of the primary conundrums inherent in restitutionary claims – namely, that while restitution is partially equitable in nature and “is the one aspect of our legal system that makes a direct appeal to standards of equitable and conscientious behavior”,<sup>39</sup> it is nevertheless necessary to attempt to identify the legal boundaries of restitutionary liability so that the law of restitution does not devolve into a vast category of cognizable claims based merely in morality rather than “the question of legal obligation.”<sup>40</sup> However, the power of restitutionary theory lies precisely in its reliance on “general principles”; as commentators have noted, while such legal quandaries concerning the precise limitations of specific causes of action exist in other areas of the law, “restitution claims generate problematic cases more frequently.” Certainly, a dose of legal realism requires an acceptance that such “troublesome cases will result from both the indeterminacy of rules and from the want of comprehensiveness in any set of rules -- conditions from which no escape is either possible or desirable.”<sup>41</sup> Utilizing general principles of restitution allows for recovery in

---

<sup>37</sup> Restatement (First) of Restitution § 1, cmt. b (1937).

<sup>38</sup> While the Restatement of Restitution primarily considers the benefit obtained by a defendant, the Restatement of Contracts recognizes two means of measuring restitution: first, the reasonable value of what the plaintiff gave to the defendant and second, the increase in the defendant’s property or interests. *See* Restatement (Second) of Contracts § 371 (1981).

<sup>39</sup> Restatement (Third) of Restitution and Unjust Enrichment § 1 (Tentative Draft 2004).

<sup>40</sup> *Id.*

<sup>41</sup> Restatement (Second) of Restitution § 1, cmt. d (Tentative Draft No. 1 1983).

cases, such as data mishandling scenarios, wherein corporate practices may otherwise generally escape public notice or accountability.

Of course, there are a limited number of alternative legal methods -- primarily statutory -- by which to reach such third party actors. For example, under the federal Fair Credit Reporting Act, an individual may sue a credit reporting agency such as Experian or Equifax for providing information to a party who does not have a permissible purpose for that information -- a typical permissible party an entity or individual such as a creditor, insurer, employer or landlord.<sup>42</sup> Another example is that under Section 5(a) of the Federal Trade Commission Act,<sup>43</sup> unfair and deceptive trade practices in commerce are prohibited. Thus, companies can be held liable for using personal data in ways that violate the express provisions of their privacy policies or statements made to consumers. Finally, state laws might provide stronger information privacy protection than federal statutory or common law.<sup>44</sup>

---

<sup>42</sup> Federal Trade Commission, *A Summary of Your Rights Under the Fair Credit Reporting Act*, <http://www.ftc.gov/bcp/conline/edcams/fcra/summary.htm> (last accessed on September 13, 2004).

<sup>43</sup> 15 U.S.C. § 45(a)(1) (“unfair or deceptive acts or practices in or affecting commerce are declared unlawful”). Unfair practices are those that “cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C. § 45(n). The determination of whether a trade practice is unfair or deceptive is made through the FTC’s administrative process, and if FTC may seek judicial remedy of such practices through civil penalties as well as through preliminary or permanent injunctions.

<sup>44</sup> See, e.g., California Constitution, Article 1 (giving individuals the “inalienable right” to privacy). However, “California is one of the few states to have a constitutional provision on privacy and is unique in the application of that provision to the private sector.” Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 *Hastings L.J.* 877, 895 (2003). Another example is that California statutory law “requires companies and state agencies to notify California residents of certain security breaches that could result in identity theft. The law requires notice if an unauthorized person has acquired an individual’s name and either Social Security number, driver’s license number, or financial account number. The notice gives an individual the chance to take steps to protect against identity theft, such as putting a fraud alert on credit files.” *ScamSafe: California’s 2003 Law for Consumer Security*, [http://www.scamsafe.com/scamsafe/2004/03/californias\\_200.html](http://www.scamsafe.com/scamsafe/2004/03/californias_200.html) (last accessed on September 13, 2004) (citing Civil Code §§ 1798.29 and 1798.82-1798.84 (2003)). Various state laws may also provide protection against unfair and deceptive trade practices. See, e.g., Cal. Business and Profession Code § 17200, et seq.; New York General Business Law § 349. See also Revised Uniform Deceptive Trade Practices Act (1966).

Restitution, however, is particularly well suited for the type of third-party offender cases discussed in this piece, and, as I will discuss, it has significant advantages over the traditional legal options.

#### b. Imposing Restitutionary Liability on Shadow Offenders

In cases imposing liability upon shadow offenders for improper handling or use of private data, restitution would constitute both the source of liability and the basis of remedy. Liability in such cases would be imposed not for mere use of that data, but rather, for the mishandling and misuse of that data and the improper benefits that accrue.

Significantly, as discussed, there is no requirement that a defendant acted wrongfully or tortiously in restitution cases, because “[t]he basis of a liability in restitution is that the defendant has been enriched without legal justification at the expense of the plaintiff; it is not that defendant has necessarily done anything wrong.”<sup>45</sup> As a practical matter, however, recovery in cases wherein data trafficking companies merely use and aggregate data in the normal course of business might prove more difficult, given the relatively wide latitude such companies are given in regard to utilizing personal data in commercial manners.<sup>46</sup> The challenge is in showing some benefit to defendants that a court is prepared to recognize as “unjust”; in cases of mishandling, misuse, careless use, and similar situations in which personal data can be shown to have

---

<sup>45</sup> Kull, *supra* note 33, at 17.

<sup>46</sup> *Cf.* Douglas Laycock, *The Scope and Significance of Restitution*, 67 Tex. L. Rev. 1277, 1289 (1989) (“the judicial reaction to the underlying wrong surely affects the choice of remedy.”)

been improperly safeguarded or handled, a court is arguably more likely to find such unjust enrichment on the part of defendants.<sup>47</sup>

As recovery in these shadow offender cases, defendants would pay in restitution to the plaintiff the extent to which the defendant profited or benefited from the data of the plaintiff.<sup>48</sup> For instance, in the case of the Acxiom hacking example introduced at the outset of this paper, the hypothetical plaintiffs would argue that Acxiom's use of their personal data constituted "the receipt of an economic benefit under circumstances such that its retention without payment would result in the unjust enrichment of the defendant at the expense of the plaintiff."<sup>49</sup> Acxiom's failure to properly secure and safeguard the personal data of an untold number of individuals would constitute the basis of the restitutionary claim. Similarly, in the Torch Concepts case, Torch Concepts' mistreatment of the personal data of the JetBlue passengers would form the basis for a restitutionary claim. In other words, in all such cases of improper data safeguarding, individuals whose personal data was mishandled or misused by a third party company would argue that it would constitute unjust enrichment to allow the defendant to have created the situation which gives rise to the misuse of data, to benefit from that situation, and leave the individuals empty-handed. This is true even if the consumer was not harmed in any demonstrable manner.

---

<sup>47</sup> See Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 Geo. L. J. 2029, 2034 (2001) (noting that "the harvesting of private information is driven by both market and Enlightenment ideologies" but that such harvesting has limits in a society which "has determined that the common good requires limits on the profit-seeking behavior of private entities.")

<sup>48</sup> See *infra*, Part II, section d ("Calculating Recovery").

<sup>49</sup> Restatement (First) of Restitution § 1 (1937).

Again, the focus is not merely on the fact that the defendant was enriched at the expense of the plaintiff, but specifically on the fact that the defendant was enriched under circumstances that are deemed unjust.

Crucially, it is largely irrelevant whether the “first party actor” in such cases (oftentimes the retail or service company that compiled their consumers’ data in the first instance) may be held liable for improper or deceptive use of consumer data. In many cases, such actors will be in privity of contract with the consumer. Certainly, claims based on breach of contract may prove successful against such companies for using personal data in a manner that runs afoul of the contract between the company and the individual.<sup>50</sup> However, companies easily escape exposure to such claims of contractual breach by, for example, simply altering their privacy policies<sup>51</sup> or limiting statements regarding their use of personal customer information. Moreover, a restitutionary remedy levied against third-party shadow offenders is powerful precisely because it also seeks to place accountability for improper use of personal data at the doorsteps of the broader cluster of companies involved in data mishandling, rather than myopically focusing on the obvious candidate for liability -- namely, the company that originally collected the data from the individual. For example, in the consolidated class action lawsuit filed

---

<sup>50</sup> For example, in the consolidated class action suit against JetBlue, plaintiffs allege that:

“JetBlue maintains on its website a clear privacy policy . . . JetBlue specifically represents that any financial and personal information collected by JetBlue ‘is not shared with any third parties, and is protected by secure servers,’ and also claims to have in place security measures to protect against the loss, misuse and alteration of consumer information under JetBlue’s control . . . Despite these self-imposed public assurances that created an obligation . . . not to act in derogation of JetBlue’s privacy policy and to refuse to share personal and financial information it collected, in September 2002, JetBlue turned over passenger information to Torch Concepts. . . Notably, prior to turning over such data, JetBlue failed to obtain the authorization or consent of passengers necessary under its privacy policy. . .”

Consolidated Class Action Complaint, *In re JetBlue Privacy Litigation*, 2004 WL 578605 (February 4, 2004).

<sup>51</sup> See *infra*, note 60.

against the cluster of corporate actors in the JetBlue case, plaintiffs have alleged, *inter alia*, unjust enrichment not only by Torch Concepts, Acxiom, and the company that allegedly subcontracted the profiling study at issue in the case, but also by JetBlue, the company that collected the data in the original instance and shared it with these third-party companies.<sup>52</sup> In this and similar cases, liability may be certainly alleged against “first-party” companies on the basis of a myriad of alternative claims, including unjust enrichment. Yet the power of allowing restitutionary recovery against the companies with whom the data was shared is that it allows for the possibility of redressing the problem of personal data abuse at every level of the data trafficking industry, rather than merely reaching the usual and most obvious suspects.

### c. The Advantages of the Restitutionary Approach

The restitutionary remedy is particularly well suited to these third-party data offenses, and in particular, it has distinct advantages over some of the other possible approaches.

First, the restitutionary approach properly encourages third party data traffickers to prevent mishandling of data. Restitution, in general, “seeks to punish the wrongdoer by taking his ill-gotten gains, thus removing his incentive to perform the wrongful act again.”<sup>53</sup> In shadow offender cases, a restitutionary remedy that looks to the amount to which a company is unjustly enriched is more likely to act as a powerful disincentive vis-

---

<sup>52</sup> See Consolidated Class Action Complaint, *In re JetBlue Privacy Litigation*, 2004 WL 578605 (February 4, 2004).

<sup>53</sup> Am. Jur. §35, *Difference Presented When Restitution Sought – Damages* (2003).

à-vis the counteracting profit incentive that leads to cavalier data treatment, inasmuch as it leads to corporate internalization of the costs of data mishandling.<sup>54</sup>

Second, a restitutionary remedy goes beyond causes of action based in a promise – such as breach of contract, fraudulent misrepresentation, or deceptive trade practices – all of which rely on a claim that a company handled one’s data in a way that it said it would not do.<sup>55</sup> As an example, in the JetBlue/Torch Concepts case, the Electronic Privacy Information Center has complained to the FTC about the actions of both JetBlue and Acxiom<sup>56</sup> pursuant to the provisions of the Federal Trade Commission Act, which prohibits unfair and deceptive trade practices;<sup>57</sup> EPIC essentially alleges that both companies disclosed passenger’s data after saying that they would not. Similarly, a consolidated class action suit has been filed against JetBlue on the grounds of breach of contract and unfair and deceptive trade practices.<sup>58</sup> In effect, the aggrieved passengers argue that JetBlue breached its privacy policy inasmuch as the company promised not to do precisely what it did – disclose passengers’ personal data.

In contrast, a restitutionary claim is not based in promise, and therefore does not rely on the presumption that a company has made a specific set of promises before

---

<sup>54</sup> Cf. Samuelson, *supra* note 16, at 1128-29 (“a property rights model [of information privacy] would force companies to internalize certain social costs of the widespread collection and use of personal data now borne by others.”)

<sup>55</sup> “The unjust enrichment claim in the context of a contract implied in law does not depend in any way upon a promise or privity between the parties.” *University of Colorado Foundation*, 342 F.3d at 1309 (quoting *Wistrand v. Leach Realty Co.*, 364 P.2d 396, 397 (1961)). A cause of action based in unjust enrichment “arises ‘not from consent of the parties, as in the case of contracts, express or implied in fact, but from the law of natural immutable justice and equity.’” *Id.* (quoting *DCB Construction Co. v. Cent. City Dev. Co.*, 965 P.2d 115, 119 (Colo.1998)).

<sup>56</sup> Electronic Privacy Information Center’s Complaint Against JetBlue Airways and Acxiom Corp. to the Federal Trade Commission, September 22, 2003, <http://www.epic.org/privacy/airtravel/JetBlue/ftccomplaint.html>.

<sup>57</sup> Numerous state laws also provide protection against unfair and deceptive trade practices. See *supra* note 44.

<sup>58</sup> See Consolidated Class Action Complaint, *In re JetBlue Privacy Litigation*, 2004 WL 578605 (February 4, 2004).

liability can be found. In many cases, of course, the contractual relationship regarding informational privacy existing between a company and its customers is governed merely by a privacy policy drafted by the company; such policies “often simply serve to notify individuals of the control that they do not have”<sup>59</sup> and are easily modified in order to provide an ever-increasing amount of data use by companies.<sup>60</sup> To the contrary, restitutionary liability is based on the idea of unjust enrichment rather than a set of broken promises.

Thus, it would be possible to reach one of the primary actors in the incident, Torch Concepts, because there is no hurdle of first finding some explicit promise made and then broken.

Third, a restitutionary remedy similarly allows us to move beyond causes of actions for personal data use based in tort – such as misappropriation of name and likeness<sup>61</sup> – which have met with little success in the courts. Of course, in some restitution cases liability arises because the defendant has accrued some benefit through the commission of a tort. However, commission of a tort is not a requisite for a restitutionary claim.

---

<sup>59</sup> Cohen, *supra* note 47, at 2041.

<sup>60</sup> However, in a recent FTC action brought pursuant to Section 5 of the Federal Trade Commission Act, Gateway Learning Corporation entered into a proposed settlement of charges that it retroactively changed its privacy policy without the notice or consent of its customers. Under the terms of the settlement Gateway would be barred from making such unilateral changes to its privacy policy. The FTC states that this is the “first FTC case to challenge deceptive and unfair practices in connection with a company’s material change to its privacy policy.” Federal Trade Commission Press Release, *Gateway Learning Settles FTC Privacy Charges*, July 7, 2004, <http://www.ftc.gov/opa/2004/07/gateway.htm>. See also Decision and Order in the Matter of Gateway Learning Corp., FTC Docket No. C-4120, September 10, 2004, <http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf>.

<sup>61</sup> See, e.g., Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 N.W. U. L. Rev. 63, 69 (2003) (arguing for the utilization of the tort theory of misappropriation “as one way to address invasive consumer data profiling. Appropriation provides for liability against one who appropriates the identity of another for his own benefit, which is nearly always a commercial benefit.”) See also Joel Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 Hastings L.J. 877, 893-94 (2003).

Fourth, most of the harm from lapses in personal data security – which takes the practical form of societal problems such as fraud and identity theft – currently falls on the consumer. Hence, one of the added benefits of a restitutionary remedy is that it obtains a tangible remedy for the individual victim; in contrast, public remedies such as the Federal Trade Commission Act often result in remedies that fail to directly compensate the victims, such as civil penalties<sup>62</sup> collected by the FTC, preliminary or permanent injunctions,<sup>63</sup> and settlements that result in prospective remedial actions such as strengthening security measures or agreeing not to engage in similar behavior in the future.<sup>64</sup>

---

<sup>62</sup> The dearth of instances of direct consumer redress is not limited to the information privacy realm; critics of the recent tobacco industry settlements argue not only that victims of the tobacco industry have gone uncompensated, but also that states are using tobacco settlement proceeds inappropriately and in ways that fail to aid individual victims. *See, e.g., Tobacco Money-Use Blasted; A Whistle Blower Said the State Committed Moral Treason in its Use of its Settlement*, Orlando Sentinel, at B5, February 11, 2004 (2004 WL 67242673) (“former tobacco executive . . . says Florida's government is committing ‘moral treason’ by using almost all of its tobacco-settlement money on programs not aimed at reducing tobacco use.”) *See generally* Susan Beck, *The Lobbying Blitz Over Tobacco Fees*, The Legal Times, January 6, 2003, at 1.

<sup>63</sup> Of course, in a consumer redress action, the FTC may seek redress for the injured parties by way of “judicial imposition of relief as the court finds necessary to redress injury to consumers or other persons, partnerships, and corporations resulting from the rule violation or the unfair or deceptive act or practice, as the case may be. Such relief may include, but shall not be limited to, rescission or reformation of contracts, the refund of money or return of property, the payment of damages, and public notification respecting the rule violation or the unfair or deceptive act or practice, as the case may be.” 15 U.S.C. § 57b. However, the FTC frequently enters into settlements that bypass consumer redress altogether. *See infra* note 64.

<sup>64</sup> For example, in a recent FTC action, Tower Records “agreed to settle Federal Trade Commission charges that a security flaw in the Tower website exposed customers’ personal information to other Internet users, in violation of Tower’s privacy policy representations and federal law.” Federal Trade Commission Press Release, *Tower Records Settles FTC Charges*, April 21, 2004, <http://www.ftc.gov/opa/2004/04/towerrecords.htm>. *See also* Decision and Order, *In the Matter of MTS Inc. d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004) <http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf>. Rather than obtaining redress for the specific individuals harmed by the data exposure, “[t]he settlement . . . bar[s] misrepresentations in the future, require Tower to implement an appropriate security program, and require audits of its Web site security every two years by a qualified third-party security professional for ten years.” Federal Trade Commission Press Release, *Tower Records Settles FTC Charges*, April 21, 2004, <http://www.ftc.gov/opa/2004/04/towerrecords.htm>. Similarly, in an FTC action against Gateway Learning Corporation which alleged unfair and deceptive practices in Gateway Learning’s use of personal information and in its retroactive modification of its privacy policy, *see supra* note 60, the monetary damages of \$4,608.00 imposed on Gateway were disgorged to the United States Treasury. This disgorgement amount represented Gateway’s earnings from improperly renting out its customers’ personal

Fifth, a restitutionary remedy avoids the difficulty of trying to place an inherent value on personal data or compute the precise mathematical value of one's own personal information. Rather, a court would calculate "value" based on what the defendant gained -- for example, the extent to which an information database company is unjustly enriched by selling personal information. And this also, interestingly, also enables avoidance of the problems inherent in attempting to treat personal data as property. The leading critics of such an approach have argued that attempting to treat personal data as property is misguided, first, because it leads to jurisprudential roadblocks such as the commodification of personal data and second, because it encounters practical roadblocks such as the likelihood of inefficient and expensive bargaining over specific rights to personal data.<sup>65</sup> Restitution allows us to analyze the benefits, profits or other advantages procured from data, rather than the precise value of individual data fragments. Indeed, the nullification of profits and ill-gotten gains is the aspect of the restitutionary remedy that could prove so powerful in the rebalancing of power in the privacy wars between consumers and corporations.

#### d. Calculating Recovery

In these shadow offender cases, recovery should be measured by the benefit to the defendant and should take the form of monetary compensation. Certainly, recovery could be measured by the pecuniary advantage gained from use of the plaintiff's data.

---

information. The customers whose personal data was sold therefore received no personalized remedy in the case.

<sup>65</sup> See generally Pamela Samuelson, *Privacy as Intellectual Property*, 52 Stan. L. Rev. 1125 (2000); Jessica Litman, *Privacy and E-Commerce*, 7 B.U. J. Sci. & Tech. L. 223 (2001).

However, recovery need not be measured in terms of direct monetary gain;<sup>66</sup> restitutionary recovery may also be measured by some other gain or benefit. For example, in the Torch Concepts case, Torch arguably benefited from the use of the personal data of JetBlue passengers in ways other than direct pecuniary profit; for example, based on the passenger data, it was able to build a proprietary terrorism risk assessment model. Here, Torch's ultimate benefit may have been monetary, but its immediate and direct benefit might also be calculated by reference to the increase in the value of its intellectual property portfolio, which now encompasses the unique model made possible only by access to the JetBlue passenger data.

Restitutionary recovery would prove especially fruitful to plaintiffs in these data mishandling cases because they are cases in which "plaintiff's damages are hard to measure and defendant's profits are clear"<sup>67</sup>. . . In such cases, restitution of defendant's profits has sometimes been thought of as a proxy for plaintiff's losses. But restitution of the profits is available even when they bear no relation to plaintiff's losses."<sup>68</sup> Thus, for example, while a victim of improper data sharing may not be able to prove her damages, it may be easy to measure the defendant's profit from use of the plaintiff's data. In the Acxiom and Torch Concept cases discussed above, the damages to the data victims might be enormous, but these are exemplary cases of the difficulty of establishing the harm that results from personal data abuse at the hands of corporations, and therefore paradigmatic examples of the potential applications of restitution.

---

<sup>66</sup> Restatement (First) of Restitution § 1, cmt. b (1937).

<sup>67</sup> Analogously, Judge Posner has explained that in copyright infringement cases, "[b]y preventing infringers from obtaining any net profit it makes any would-be infringer negotiate directly with the owner of a copyright that he wants to use, rather than bypass the market by stealing the copyright and forcing the owner to seek compensation from the courts for his loss. Since the infringer's gain might exceed the owner's loss, especially as loss is measured by a court, limiting damages to that loss would not effectively deter this kind of forced exchange." *Taylor v. Meirick*, 712 F.2d 1112, 1220 (7<sup>th</sup> Cir. 1983).

<sup>68</sup> Laycock, *supra* note 46, at 1287.

These shadow offender cases have the unique characteristic of, by and large, constituting cases wherein the plaintiff's losses and the defendant's gains will often be disproportionate.<sup>69</sup> In this way, they are analogous to intellectual property restitution cases, wherein "[t]he most controversial cases arise when the property produces gains to the defendant that clearly exceed plaintiff's losses. The property might change in value so that it is more valuable in defendant's hands, or simply more valuable at the time of trial, than it was in plaintiff's hands before the wrongful transfer. Or the defendant may put the fruits of his wrong to some profitable use, earning consequential gains that exceed plaintiff's consequential losses."<sup>70</sup> In data mishandling cases, as in these intellectual property restitution cases, "[r]estitution as a measure of recovery matters precisely when defendant's gain exceeds plaintiff's provable loss, either because plaintiff's loss is small or because it is hard to prove."<sup>71</sup>

On the opposite spectrum, plaintiff's losses may be high, but the defendant's gains are arguably disproportionately low, because the defendant's gain from that particular plaintiff's specific data is an infinitesimal portion of the benefit derived by the

---

<sup>69</sup> Indeed, as the drafters of the Restatement (Second) of Restitution explained, "[c]ases of matching gain and loss are . . . only a limited class of the applications of contemporary restitution law. The principles stated in [the Restatement] incorporate not only factors of gain and loss, but also factors of fault and mistake, of inducement and reliance, and of motivation." Restatement (Second) of Restitution, Introductory Note (Tentative Draft No. 1 1983).

<sup>70</sup> Laycock, *supra* note 46, at 1287.

<sup>71</sup> *Id.* Thus, for example, in *LinkCo, Inc. v. Fujitsu Ltd.*, 232 F.Supp.2d 182 (S.D.N.Y. 2002), the court explained that in cases of misappropriation of trade secrets, recovery may be calculated by reference to plaintiff's losses or defendant's unjust enrichment; in addition, where these calculations "provide inadequate compensation to the plaintiff," recovery may be calculated based on a "reasonable royalty", *i.e.*, "what the parties would have agreed to as a fair licensing price." *Id.* at 186. The royalty measure of damages "attempts to measure a hypothetically agreed value of what the defendant wrongfully obtained from plaintiff." *Id.* at 186 (quoting *Vermont Microsystems, Inc. v. Autodesk, Inc.*, 88 F.3d 142, 151 (2d Cir. 1996)). While this "reasonable royalty" calculation would be unavailable to plaintiffs in personal information mishandling cases because personal information is not deemed "property" subject to the laws of intellectual property, such a calculation echoes the basis of recovery in unjust enrichment, inasmuch as it seeks to recoup wrongfully obtained benefits. Indeed, in trade secret misappropriation cases, courts have determined that "the lack of actual profits does not insulate the defendants from being obliged to pay for what they have wrongfully obtained." *Id.* (quoting *University Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 536 (5<sup>th</sup> Cir. 1974) (citing *In re Cawood Patent*, 94 U.S. 695 (1876))).

defendant. Of course, in a class action suit, the aggregate benefit might be quite large, but even in the case of an individual plaintiff, a jurisprudential basis for adequate recovery exists. Significantly, when “the defendant was tortious in his acquisition of the benefit”<sup>72</sup> the law of restitution allows plaintiffs to recover their losses rather than the defendants’ gain.<sup>73</sup> In addition, a defendant must also pay all profit derived from the benefit if it was “consciously tortious”<sup>74</sup> or intentionally acted wrongfully<sup>75</sup> in acquiring the benefit. Therefore, victims of data misuse and mishandling might be able to recover the amount of their losses and possibly all of defendant’s profits where the defendant acted tortiously in acquiring the benefit. For instance, a plaintiff might argue that Torch Concepts acted tortiously in the JetBlue case by going above and beyond the purposes intended by the government in the original national defense project. If she could prove these facts, recovery for her losses -- such as losses resulting from damages caused by being identified as a terrorist risk -- might be allowable.

This solution to the problem of disproportionately high losses in regard to defendants’ gain, however, relates to the crucial quandary in the question of recovery: is recovery appropriate in cases wherein the defendant is not directly enriched by the mishandling of the data, for example, in cases of hacking? Thus, for example, in the

---

<sup>72</sup> Restatement (First) of Restitution § 155 (1937). See also Restatement (First) of Restitution I, 8, 2, Intro. Note (1937); *Olwell*, *supra* note 36, at 287, 654.

<sup>73</sup> See Restatement (First) of Restitution § 155 (1937). For example, in a case where the plaintiff repaired defendant’s boat engines to the benefit of defendants, the court held that while the plaintiff was “entitled to recover the benefit he bestowed under a quasi-contract theory,” no evidence was shown that “any tortious conduct on the owners’ part caused them to receive the benefit”; the court determined that in such cases wherein the defendant did not tortiously acquire the benefit, “the measure of recovery is the value of what was received” rather than loss or cost to the plaintiff. *Kane v. Motor Vessel Leda*, 355 F. Supp. 796, 801 (E.D. La. 1972) (quoting Restatement (First) of Restitution § 155 (1937)).

<sup>74</sup> Restatement (First) of Restitution § 155 (1937).

<sup>75</sup> See Restatement (Third) of Restitution & Unjust Enrichment § 3 (Tentative Drafts 2004).

Acxiom case, Acxiom ostensibly did not receive a “benefit” from the hacking of its databases.

Data traffickers are, of course, sometimes directly enriched from mishandling of consumer data; for example, where a credit reporting agency shares a consumer’s personal data cavalierly because it profits by doing so,<sup>76</sup> and a case of identity theft results. Here, the improper handling of the data and the defendant’s enrichment go hand-in-hand.

But even where these two – the mishandling of the data, on the one hand, and the enrichment of the defendant, on the other – are not the foreseeable pattern of events, that is, are not the necessary cause and effect, a broader view of the proper limits of restitution is necessary. In all of these cases, the improper handling of personal data is tied to and inherently bound up with the benefit to the defendant. The personal data of an individual has directly conferred an advantage on the data trafficking company in these cases, and because the individual’s data was mishandled in a way that leaves her disadvantaged and in a worse position, the law of restitution should deem the retention of that advantage without payment under such circumstances to be unjust.<sup>77</sup>

---

<sup>76</sup> See, e.g., *TRW Inc. v. Andrews*, 534 U.S. 19 (2001) (wherein credit reporting agency disclosed a consumer’s credit report to several companies at the request of an imposter attempting to establish credit in the plaintiff’s name, and the plaintiff alleged that the credit reporting agency failed to engage in the requisite verification procedures to ensure that the plaintiff had initiated the request).

<sup>77</sup> As discussed *supra*, while such a direct connection is not a requisite for a restitutionary cause of action, it may impact the level of recovery because “the more culpable the defendant’s behavior, and the more direct the connection between the profits and the wrongdoing, the more likely that plaintiff can recover all defendant’s profits.” *University of Colorado Foundation, Inc. v. American Cyanamid Co.*, 342 F.3d 1298, 1311 (Fed. Cir. 2003). See also Laycock, *supra* note 46, at 1289 (“The more culpable defendant’s behavior, and the more direct the connection between the profits and the wrongdoing, the more likely that plaintiff can recover all defendant’s profits.”)

## Conclusion

The restitutionary remedy argued for here is not without practical and jurisprudential limitations. It assumes some unfair quality to the nature of the relationship between the defendant and the plaintiff, such as a company profiting from use of an individual's data while, at the same time, failing to ensure adequate security measures or failing to prevent cavalier treatment of that data. It therefore does not reach those cases that do not involve improper handling of data. Hence, this paper implicitly assumes that separate normative questions must be asked about the generalized use of personal data that does not fall within the category of "bad actor" cases. Similarly, while the restitutionary remedy certainly incentivizes data mishandlers to safeguard individuals' data privacy,<sup>78</sup> it is arguably merely a backend measure that operates as a sort of a tax on bad actors rather than a front-end, prohibitive measure that would operate as a more complete safeguard against privacy abuses.

Nevertheless, restitution is a promising remedy because it would strongly incentivize such third party companies to properly safeguard personal information where, traditionally, few such incentives have existed. Moreover, as I have argued, such a remedy allows us to move beyond the problems associated with purely public remedies, causes of action based solely in contract, and the inherent difficulties of placing monetary value on personal data.

---

<sup>78</sup> Commentators have similarly argued that the use, aggregation and distribution of personal data by data trafficking companies "creates externalities, or costs borne by others. Externalities are created when a person engages in an activity that imposes costs on others but is not required to take those costs into account when deciding whether to pursue the activity. The feelings experienced by consumers whose information is sold and used against their wishes constitute just such externalities." Jeff Sobern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 Wash. L. Rev. 1033, 1106 (1999).