Volume 41
Number 3 *Spring 2007*

*pp.*1061-1142

Spring 2007

Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation

Elizabeth De. De Armond

Articles

FROTHY CHAOS: MODERN DATA WAREHOUSING AND OLD-FASHIONED DEFAMATION

Elizabeth D. De Armond*

I. INTRODUCTION

Every individual is unique. Each of us has a unique set of facts that positively distinguishes us from everyone else in the world.[1] Even identical twins develop a different history, a different biography of events, over the course of time. Among these events are our transactions in commerce—the accounts we open, the items we buy, the bills we pay, the services we obtain, the charges we make. All of these events can now be, and often are, recorded digitally so that they can easily be duplicated, searched, and transmitted to others. These advances in information technology have not only benefited traditional entities that aggregate personal information, such as credit reporting agencies, but new aggregators who collect all sorts of information about individuals and warehouse it in databases, and "data miners" who analyze and assemble disparate bits of information about individuals to assemble profiles of behavior.

In the midst of all this personal information churns a wealth of false information, transactions linked to the wrong actor. Some of the misattribution arises from identity theft, allowing impostors to pose as their victims to gain goods and services. However, the detachment of individuals from their data raises the real risk that one person's deed will be mismatched to another person's identity, even when no thief has sought to intentionally misdirect information. Our failure to take care to match events with identities has led to a "frothy Chaos" of misinformation and mismatched transactions.[2] Furthermore, the power of mismatched information, especially about financial transactions, to disrupt or even paralyze, the lives of individuals has grown dramatically. Important decisions are made based on rumor rather than

* Assistant Professor of Law, Legal Research and Writing, Chicago-Kent College of Law. I would like to thank Kristen Osenga and participants at a faculty workshop at Chicago-Kent for their valuable comments on an earlier draft of this Article.

1 ERVING GOFFMAN, STIGMA: NOTES ON THE MANAGEMENT OF A SPOILED IDENTITY 57 (1963).

2 Michel Eyquem de Montaigne, *Of Glory*, *in* ESSAYS 565 (John Florio trans., 1904).

fact—defamation of a most damaging sort, damaging to reputation, damaging to personality, and damaging to dignity.

Nonetheless, the power of law to curb the creation of these flawed links has not kept up with information technology and its use. The main legal scheme that regulates the aggregation and reporting of personal financial information, the Fair Credit Reporting Act ("FCRA"), has failed to maintain the integrity of that information, leading to too many individuals suffering from a false reputation tainted by the acts of others.[3]

However, the information age has not just given us the power to record, store, and disseminate data; it allows us to use computers to analyze, cross-check, and verify data more easily. These tools can identify inaccurately-attributed information and keep it out of the data sea. The age old tort of defamation, when viewed in light of these new processes, can allow realistic relief that may motivate data aggregators to treat individual records and personal identifying information much more carefully.

In Shakespeare's *King Richard II*, loyal Thomas Mowbray alludes to the distinction between a "spotless reputation" and the body that it is connected to.[4] We may not all have spotless reputations, but we are at least entitled to the reputation deserved by our own deeds rather than the deeds of someone else. The answer to the problem of misinformation about individuals lies not in retreating from technology, but in embracing it.

This Article examines the particular problem of data inaccuracies caused by or aggravated by information technology, the impact such data can have on consumers, and the opportunity for the traditional tort of defamation to redress that impact. Part II of this Article describes how

---

3 Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (2000) [hereinafter FCRA].

4 WILLIAM SHAKESPEARE, THE TRAGEDY OF KING RICHARD II act 1, scene 1 (3d ed. 2000). The full quotation is as follows:

> The purest treasure mortal times afford
> Is spotless reputation. That away,
> Men are but gilded loam or painted clay.
> A jewel in a ten-times-barred-up chest
> Is a bold spirit in a loyal breast.
> Mine honor is my life, both grow in one;
> Take honor from me, and my life is done.
> Then, dear my liege, mine honour let me try;
> In that I live and for that will I die.

Id.

individuals' transactional identities develop through the aggregation of individual events and identifies the entities that provide, collect, and analyze those records. It then discusses the problem of false data, especially false financial data, and explains how current information practices have increased the power of such dirty data over the dignity and personhood of individuals. Part III describes the FCRA, the existing legal structure that should protect individuals from the impact of such bad data, and how it has failed. Part IV identifies how the common law tort of defamation can be brought up to date to appropriately balance the rights and needs of individuals to bear an accurate reputation and the power of data warehousers and miners over the vast databases they tend.

II. THE PROBLEM

A. Biography and Image: The Construction of Our Transactional Identity

John Locke once described the identity of any one person as consisting of "nothing but a participation of the same continued Life, by constantly fleeting Particles of Matter, in succession vitally united to the same organized Body."[5] Throughout our continued lives, we participate in any number of events and transactions, performing all sorts of deeds. Many of these are transactions where we exchange money or the promise to pay money for goods and services or, in the case of charity, for some higher return. For any one person, a full biography of these transactions with others will distinguish that individual from every other.[6]

Once, these transactions would have remained inseparable from the parties who made them. In a local economy, a merchant would have known his customers and a banker would have known his borrowers, by name and by face. Reputations would have been built from these face-to-face transactions. Many transactions would have left no physical record behind, but when Locke wrote these words in 1690 some might have been memorialized on paper—a loan in a ledger, a sale on a receipt. Although a particular individual would know of his own biography of transactions, any third party could compile that list only by going from store to store and bank to bank to painstakingly draw it up.

---

[5] JOHN LOCKE, AN ESSAY CONCERNING HUMANE UNDERSTANDING bk. II, ch. 27, § 6, at 331-32 (Peter H. Nidditch ed., Oxford Univ. Press 1975) (1690).

[6] *See* GOFFMAN, *supra* note 1, at 56 (describing the full set of facts known about someone as a complex that positively identifies that individual).

Because of the localized economy and in-person transactions, the chances of ascribing a particular deed to the wrongdoer were likely slight; should such an error have occurred, likely the consequences would have been circumscribed to one event and the error easily undone with a few strokes of a pen, at least so long as the one making the error did not specifically seek to defame the customer.[7] One's reputation may not have been wholly free from calumny and slander, but generally the false words would have come from someone local, who was known, who could be corrected or perhaps exposed.[8] Because the transactions were local, individuals had control over their reputations.

Now, however, instead of transacting with someone across a counter, we transact with someone across the country, or even across several continents.[9] Transactions are much more likely to be electronic and to be memorialized electronically, not just inscribed in a book. Transactions that once would have required a consumer to physically put pen to paper to sign off on an exchange can now be achieved without pen or paper.[10] We are far more likely now than a few decades ago to borrow from or spend money with an entity that never sees us. In fact, many details of a transaction might never fall in front of a pair of human eyes. For example, a lender's computer may automatically debit a borrower's bank account for the amount due monthly on a mortgage. The funds may be subtracted from the borrower's account and added to the lender's without any human intervention at all.[11] Even when a transaction does involve an interpersonal transaction, such as when a department store clerk opens a charge card account for a customer at a store counter, the details of the event will be recorded and stored in electronic form and only incidentally on paper. The rise in this sort of

---

7 R.C. Donnelly, *History of Defamation*, 1949 WIS. L. REV. 99, 100-03. The defamation cases among the local cases in the English middle ages typically concerned personal insults. *Id.*

8 *See generally* KENNETH GROSS, SHAKESPEARE'S NOISE (2001) (discussing themes of slander, rumor, and gossip in *Hamlet, Measure for Measure, King Lear,* and *Coriolanus*). Though written a bit earlier than Locke's works, many of Shakespeare's plays explored, as part of the study of the characters, their reaction to slander from familiar sources. *Id.*

9 *Cf.* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 314 (2000).

10 *See* Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001-7021 (2000); The Uniform Electronic Transactions Act § 7 (draft 1999), *available at* http://www.law.upenn.edu/bll/ulc/uecicta/eta1299.htm. Such electronic signatures can authenticate a transaction much as a written one can. Uniform Electronic Transactions Act, *supra.*

11 Electronic Funds Transfer Act, 15 U.S.C. §§ 1693-1693r (2000). Such a transaction is called a "preauthorized electronic fund transfer" and is generally governed by the Electronic Funds Transfer Act. *Id.*

electronic, detached commerce has led to a variety of federal laws to regulate it, including the Electronic Funds Transfer Act,[12] the Electronic Signatures in Global and National Commerce Act,[13] and the Check Clearing for the 21st Century Act.[14]

This change in the form of commerce has correspondingly changed the construction of each person's transactional identity, the image from which an individual's reputation flows. Through one's actions, one relates to others and makes impressions on them. These impressions, taken as a whole, constitute an individual's reputation—that is, what other people think of you, to the extent that their thoughts arise from what they know about you, or think they know about you.[15] As Steven Heyman writes, "While reputation belongs to the self, in another sense it is external to the self, existing within the minds of others."[16] Thus, our reputation for worthiness to participate in transactions depends on our transactions, the image that those transactions portray, and how others view that image.

The biography of our transactions is not fixed; it changes with each transaction, each transaction augmenting a person's history, adding to it like a flake of snow onto a snowball, compiling what Erving Goffman referred to as "a single continuous record of social facts" that stick to our identity.[17] A single day in a typical modern consumer's life could yield the information that such a consumer bought a cup of coffee and a newspaper, ate lunch out, purchased two books that were on the *New York Times* bestseller list, refilled a prescription, paid a gas bill, all added to the data sea. Each day, more and more such transactions will stick to

---

12 *Id.* §§ 1693-1693r.

13 15 U.S.C. §§ 7001-7021 (2000).

14 12 U.S.C. § 5001 (Supp. III 2003) (allowing banks to substitute an electronic image of a check for the paper item through the electronic process). *See generally* BENJAMIN GEVA, THE LAW OF ELECTRONIC FUNDS TRANSFERS (2002).

15 *See* THE NEW SHORTER OXFORD ENGLISH DICTIONARY ON HISTORICAL PRINCIPLES 2556 (1993) (listing as one definition of "reputation": "[t]he general opinion or estimate of a person's character, behaviour, etc.; the relative esteem in which a person or thing is held"); Lawrence M. Friedman, *Name Robbers: Privacy, Blackmail, and Assorted Matters in Legal History*, 30 HOFSTRA L. REV. 1093, 1094 (2002).

16 Steven J. Heyman, *Righting the Balance: An Inquiry into the Foundations and Limits of Freedom of Expression*, 78 B.U. L. REV. 1275, 1325 (1998). "In this way, [according to Heyman,] reputation resembles the right to property, which is also external to the individual." *Id.*; *see also* Montaigne, *supra* note 2, at 560 ("There is both name, and the thing: the name, is a voice which noteth, and signifieth the thing: the name, is neither part of thing nor of substance: it is a stranger-piece joyned to the thing, and from it.").

17 GOFFMAN, *supra* note 1, at 57.

that individual's identity and adjust the existing image that the biography portrays.

In pointed contrast, our identifying markers are relatively fixed. Some types of identifying information—one's date of birth, place of birth, and mother's maiden name, for example—never change.[18] Social security numbers and gender have similar staying power for the vast majority of us.[19] Other forms of identifying information, such as address and telephone number, may change from time to time, more for some than for others, but generally remain stable for at least some period.

When a financial event becomes recorded electronically, markers that purport to identify a flesh and blood individual are recorded with it. This identifying information in an electronic record can be thought of as "header" information.[20] Biographies can be formed by amassing the scattered and strewn records that have matching header information. So, for example, a restaurant may record the items a customer ordered and the amount paid (including tip), tag it with header information consisting of the customer's name, and charge the account number. The record can then be pooled with other transactions bearing those markers. Similarly, a pharmacist can record the medicine, dosage, and prescribing doctor of a prescription and pair it with the customer's name, date-of-birth, and insurance information.

All of the records that bear the identity tags of a specific individual give rise to a transactional identity, what Daniel Solove calls a "digital dossier."[21] The collection of transactional identities creates a parallel universe of sorts, one inhabited by virtual individuals who comprise not Locke's "fleeting Particles of Matter," but rather permanent particles of data. This virtual person portrays its own digital reputation.[22] From the

---

[18] Concededly, one may be mistaken about such information, and new information may then change the marker.

[19] *See* The Official Website of the U.S. Social Security Administration, www.ssa.gov (last visited Jan. 13, 2007). The Social Security Administration will issue a new social security number only under very limited circumstances. *Id.*

[20] *See* Individual Reference Servs. Group, Inc. v. F.T.C., 145 F. Supp. 2d 6, 17 (D.D.C. 2001) (describing "'credit header'" information as "the name, address, social security number, and telephone number of a consumer").

[21] DANIEL J. SOLOVE, THE DIGITAL PERSON 1 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON].

[22] *Cf.* Joseph J. Beard, *Clones, Bones and Twilight Zones: Protecting the Digital Persona of the Quick, the Dead and the Imaginary*, 16 BERKELEY TECH. L.J. 1165, 1170-72 (2001) (arguing that "imaginary virtual humans," digital clones of living individuals, are entitled to protection from defamation, invasion of privacy, and commercial misassociation with products and services).

perspective of those who observe any one virtual person, whether to evaluate the person as a credit risk, an insurance or employment prospect, or someone with money to spend, the person may be no more than the particular fragments of information that interest them. The self is presented not as a unified whole, but as facets of database records.[23]

B. The Impact of Data Technology

Records of information about individuals and their transactions are not new. We have been able to track transactions since the agrarian society of the Sumerians developed Cuneiform,[24] and used it for, among other purposes, memorializing debts for barley on wet clay tablets.[25] The aggregation of transactional records is not a modern development either. Comprehensive records began to be kept to serve the needs of evolving societies in the beginning of the last millennium. For example, William the Conqueror commissioned the *Domesday Book* in 1086 to identify the ownership of all land, buildings, livestock, and other resources for the purpose of assessing taxes.[26]

But since those times, we have developed far more useful systems for recording individuals' transactions. A clay tablet is not duplicated easily, is somewhat cumbersome to carry around, and would likely be viewed by only a few people—perhaps only the original parties to the exchange. These factors constrained the power of the information on the tablet. Even access to the Domesday Book would have been limited to those with the position to gain an audience with it.

---

[23] *Cf.* Richard Warner, *Surveillance & the Self: Privacy, Identity, and Technology*, 54 DEPAUL L. REV. 847, 854-55 (2005) (describing how one's identity encompasses different social roles for different purposes).

[24] STEVEN ROGER FISHER, A HISTORY OF WRITING 26-27 (2004).

[25] Science Museum of Minnesota, http://www.smm.org/research/Anthropology/cuneiform/cuneiform.php (last visited Jan. 13, 2007) (museum cuneiform collection containing such tablets). Later, another agrarian society, the Incas, used knot records to record mercantile transactions. FISHER, *supra* note 24, at 14. The record system was known as *quipu* and continued after the Spanish conquest. *Id*. at 15. The system counted potatoes, sheep, and grains. *Id.*

[26] *See* SIR HENRY ELLIS, GENERAL INTRODUCTION TO DOMESDAY BOOK: OFFICIAL COPY FOR THE USE OF HIS MAJESTY'S COMMISSIONERS ON THE PUBLIC RECORDS OF THE KINGDOM 177 (1817). The new idea of compiled, permanent records led twelfth-century Christians to call the work the "Domesday Book," comparing it to the Last Judgment, or Doomsday, described in the Bible, when the deeds of Christians written in the Book of Life were to be placed before God for judgment. *See Revelations* 20:12, 20:15.

1. The Accessibility and Power of Data

As more of our deeds are inscribed in bytes rather than on paper, more information about us is more available and accessible than ever before. Information about individuals, from their debts to their DNA, can now be stored digitally, allowing others to duplicate, download, upload, e-mail, search, and even print the information—albeit far more likely onto paper than onto clay. Others can also compare and contrast information quickly and easily with other information and, with just a few key strokes, search the data for any string of characters.

As discussed above, all of this information about any one individual's transactions becomes a financial "digital dossier" that has replaced a locally made and personally observed reputation.[27] Now, our reputations are perceived by many observers almost entirely from bits of data over which we have practically no control. Creditors, landlords, utility companies, mortgagees, and even employers may condition services on the basis of information in an individual's credit report—the commercially available representation of a reputation—and can use that information to change the terms of a deal, or even to refuse to participate at all. A data entry thousands of miles away, created from a transaction that never involved a face, may be the single most significant piece of information to a potential creditor, employer, or government official.

It is not just the records of private sector entities, such as banks, businesses, and doctors, that have become digitized; public records are far more accessible as well. Once, to comprehensively learn someone's criminal history a researcher would have had to go to each courthouse in each jurisdiction where the target may have been and research through the public records. The information may have been public, but the pains required to search through it rendered much of it functionally invisible. However, more and more public entities record information electronically and make it available. For example, many states post online lists of sexual predators pursuant to "Megan's laws."[28] Similarly, many public records formerly buried in clerk's offices are now available via the Internet, removing the effort barrier and revealing what once would have been, for practical purposes, hidden from most.[29]

---

27 SOLOVE, THE DIGITAL PERSON, *supra* note 21, at 1.

28 *See* Doron Teichman, *Sex, Shame, and the Law: An Economic Perspective on Megan's Laws*, 42 HARV. J. ON LEGIS. 355 (2005) (listing the sex offender registry laws of all fifty states).

29 *See, e.g.*, Cook County Recorder of Deeds, http://www.ccrd.info/CCRD/il031/index.jsp (last visited Jan. 13, 2007) (property records of Cook County, Illinois). For

Public or private, much information about individuals is but keystrokes away from appearing on any computer screen in the world. Accordingly, information about an individual can be viewed by more people and more easily than can the account books of the last century.[30] Our reputations have become, as Steven Nock terms, "portable."[31] That portability has changed the power of the information.

Data in electronic form is not just much more accessible, it is also much more easily duplicated. One need not laboriously copy, character by character, information onto a new clay tablet, need not transcribe it, key by key, onto a separate sheet of paper, and need not even spin the drum of a mimeograph machine. Rather, now we can hit "control-c" and "control-v" or click "save as," and store a fresh and complete copy of the information in our own files. We can then upload that file to the Internet, making it available for one, dozens, hundreds, thousands, to likewise copy and save. Although photocopy machines also eased duplication, digital duplication allows us to send the information out in an e-mail to any number of others. Information that once was tied down, by simple physicality, to a point certain in space, can now live in a near infinite number of places.

Not only is digital information on the Internet far easier to access and duplicate than print information (or clay tablets), that access and duplicatability give it more stamina than its print cousin. Pieces of paper yellow, curl, and eventually disintegrate, and, unless catalogued with librarian-like precision, are highly likely to get lost or buried before reaching such ends. But even if many hard drives suddenly fail, an item of electronic information may well have been sufficiently copied to allow the substance to survive somewhere. Even data that a user tries to destroy often remains available to a savvy searcher.

Digital information's searchability also increases its power. Because the information resides in bytes, it sifts easily through a custom-made strainer constructed with "control-f" or a similar tool. In contrast, no control-f exists to help us find things in real space. Without the ability to have a computer search for that piece of information, the chances of recalling the data are far lower. Just as keeping records in the musty files

---

example, many taxing authorities have put property records online that list, for each parcel, that parcel's owner, the assessed value, and any interests that burden the property, such as mortgages, liens, and deeds. *Id.*

30 *See infra* text accompanying notes 31-36.

31 STEVEN L. NOCK, COSTS OF PRIVACY: SURVEILLANCE AND REPUTATION IN AMERICA 3 (1993).

of a courthouse archive room renders most of the data held within functionally invisible, material in homes, businesses, and other locales, even if exactingly indexed, will lose accessibility and with that, its power to impact future transactions.

Not only can a human easily search digitized data, but so can machines, far more quickly and thoroughly. Once programmed with a particular algorithm, a powerful computer can examine in seconds what once would have taken legions of clerks to page through. Many consumers do not realize that when they apply for credit, no one at the creditor's office may ever read the consumer's credit history. Rather, a computer will pull and examine a credit score, a number produced from that credit history through some sort of algorithm that assigns different weights to different types of data.[32] Thus, the information's power can be disconnected from the data itself, transformed via machine and algorithm into a three-digit representation of a person.

The effects of electronic storage of records and advances in database technology extend beyond increased access to and searchability of the information. The uniformity of the medium has increased the power of information because digitizing it pancakes time. Information from ten years ago might well appear just as fresh as information from yesterday. The associated aspects of aged information that might have cued us to draw less significance from it—the yellowing newspaper, the faded print, the curled and frayed edges of a long-stored document, the noir appearance of a microfiche—impacted our perception of the value of the information contained within it, and may well have led us to attribute less significance to the contents than we once would. However, these associated aspects have, in many cases, been stripped away from the content. Now, aged information may well present itself on our computer screen as being no older than, no less reliable than, no less interesting than, information dated today. We have to rely on the associated date, not other cues, to note its freshness. Thus, older information has more vigor than it once might have; therefore, we react to it differently and we give it more credence than we might have in the past. In this way, an electronic description of a past deed can have a much longer half-life than a physical record of the same event.

Additional power arises from the tremendous interest that information of the events in our lives has for those with whom we do, or would like to do, business, and for those who would like to do business

---

[32] *See infra* text accompanying notes 37-59.

with us. In the first category are those who seek to establish our merit for a specific transaction or relationship, for example, to provide us insurance, to employ us, or to extend us credit.[33] In the second are those who seek to identify us to target us for a sales pitch—direct marketers and politicians, for instance.[34] Both types assess an individual's information to determine that individual's worthiness—that is, that individual's reputation—generated from the individual data items. The appetite of these actors for our transactional information, the biography of those facts deemed relevant by others and that distinguishes us from other consumers, has grown with the ability to store those facts electronically.[35]

In light of their accessibility and vigor, these "digital dossiers" raise privacy concerns, even when they faithfully represent the deeds of the individual to which they are linked, because they impair our control over the image that we project to the world. In this conception of privacy, we have a right to a certain amount of control over the image, the face, we present to the world.[36] However, the point of this Article is not to address that duplication and distribution, the ease of access to information, as it impacts the sense of our vulnerability to true information. Rather, this Article argues that those attributions of information all magnify the importance of truth, and that importance justifies protecting individuals from bearing the burden of digital reputations poisoned by dirty data. The rate of errors and misinformation in these dossiers may be so pervasive that any single one may in fact project a fictional, "virtual" person, consisting in part of data mis-hung on the identity of the flesh and blood individual, bearing perhaps only a surface resemblance to that person. Nonetheless, no matter how poorly the universe of virtual individuals may mirror the universe of flesh and blood individuals, the world may well treat a virtual individual as more real than the flesh and blood counterpart.

---

33 *See* 15 U.S.C. § 1681a(d)(1) (2000) (providing the general definition of "consumer report" for purposes of the FCRA).

34 *See* Chris Cilliza and Jim VandeHei, *In Ohio, a Battle of Databases*, WASH. POST, Sept. 26, 2006, at A01 (discussing Republicans' use of information about voters to "microtarget" them for particular campaign material).

35 *See infra* text accompanying notes 37-59.

36 Among those who perceive privacy this way are Alan F. Westin and Thomas Nagel. THOMAS NAGEL, CONCEALMENT AND EXPOSURE 4 (2002); ALAN F. WESTIN, PRIVACY & FREEDOM 34 (1967).

2. The Big Business of Warehousing, Aggregating, and Analyzing Data

In contrast to the private-sector entities that find, analyze, and aggregate such data, individuals have very little control over their personal data.[37] The growth in the power of electronic information has sprouted entities, data aggregators, and data miners, who seek to collect the records from disparate sources, reassemble them into a digital report, and analyze them to gain a picture of that person, the image from which observers draw our transactional reputations.[38]

These modern entities have their roots in the last century. The first credit bureaus began to be organized in the late 1800s by merchants who needed to know who would repay loans and who might not.[39] Since then, however, database architecture and power have increased to allow any minute information about any commercial transaction to be recorded, compared, reassembled, and analyzed.[40] An individual's transaction history comprises all sorts of information about that individual's practices. Accounts, past and present, payments made, delayed, or missed altogether, lawsuits pending, rental history, account balances and available credit, and employment history can all be part of a credit report.[41] Unpaid parking tickets and library fines can also be

---

[37] *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1259-60 (2003) [hereinafter Solove, *Enforcing Privacy Rights*] (arguing that putting identity theft prevention on the shoulders of individuals puts the burden on the wrong parties; the security is only as good as the entities choose).

[38] See Solveig Singleton, *Privacy Versus the First Amendment: A Skeptical Approach*, 11 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 97, 126-28 (2000) (describing the aggregated information about consumer transactions as "gossip").

[39] EVAN HENDRICKS, CREDIT SCORES & CREDIT REPORTS: HOW THE SYSTEM REALLY WORKS, WHAT YOU CAN DO 177 (2d ed. 2005).

[40] Elisa Williams, *The Man Who Knows Too Much*, FORBES, Nov. 11, 2002, at 68. The Fair Isaac Corporation, for example, offers algorithms that help retailers match purchasers to other information, such as the place the purchaser lives, the car the purchaser drives, and the living the purchaser earns. *Id.*

[41] 15 U.S.C. § 1681a(d)(1) (2000). The FCRA defines a consumer report as follows:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—
>
> > (A) credit or insurance to be used primarily for personal, family, or household purposes;
> > (B) employment purposes; or
> > (C) any other purpose authorized under section 1681b of this title.

collected.[42] Experian, one of the three major consumer credit reporting agencies, advertises that it maintains more than 65 terabytes—that is, 65 trillion bytes—of data on North American consumers and businesses,[43] including details on 215 million American consumers.[44] Each of the big three credit reporting agencies receives more than 2 billion transaction records each month.[45]

But while traditional credit reporting agencies have generally kept track of consumer accounts and bill-paying practices, the modern consumer data industry has started to track far more mundane information about a person's transactions. Advances in information technology have led to an industry of "data mining," by which a miner sifts through personal information to find patterns by which to predict future behavior.[46] This industry overlaps the traditional credit reporting industry, but may collect many more types of data far beyond those arising from routine financial transactions. One example of such entities is ChoicePoint, which advertises that its database maintains information on more than 210 million individuals, from "demographic data, credit data, property and auto insurance projected renewal dates, and other insurance and financial attributes, all linked together for immediate and targeted deployment . . . ."[47] ChoicePoint offers its clients a wealth of data services, ranging from pre-employment checks and public record searches to insurance claim analyses and identity verification services.[48]

Where do these entities get these records? Well, we shed aggregatable data at every turn. We buy groceries with loyalty cards

---

Id. The definition continues to exclude certain reports from the general definition. *Id.* § 1681a(d)(2).

42 *Surprising Things Can Wreck Your Credit Score: Unpaid Parking Tickets, Overdue Library Books, Might Affect Credit* (Aug. 22, 2005), http://www.nbc10.com/consumeralert/4883326/detail.html.

43 Experian, http://www.experian.com/corporate/factsheet.html (last visited Jan. 13, 2007).

44 *Id.*

45 Robert Avery, Paul Calem, Glenn Canner, & Raphael Bostic, *An Overview of Consumer Data and Credit Reporting*, FED. RES. BULL., Feb. 2003, at 49.

46 *See* U.S. Gen. Accounting Office, No. GAO-04-548, *Data Mining: Federal Efforts Cover a Wide Range of Uses* 4 (2004), *available at* http://www.gao.gov/new.items/d04548.pdf (defining "data mining as the application of database technology and techniques–such as statistical analysis and modeling–to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results").

47 ChoicePoint, Precision Marketing, http://www.cp-pm.com/media/pdf/CPDL%20Brochure%20-%20Oct2005.pdf (last visited Jan. 13, 2007).

48 ChoicePoint, Industry Solutions, http://www.choicepoint.com/industry/all_products.html (last visited Jan. 13, 2007).

and information-ravenous merchants and marketers scoop up the records.[49] These loyalty cards can yield millions of transactions each week.[50] Every item bought can be tracked.[51] But the products we buy are not the only grist we provide to the information mill. Aggregators are also interested in the services individuals use, some of which can yield uncomfortably sensitive information as well. For example, they may want to collect the details of our cell phone calls, including the numbers dialed and the time connected.[52] The Medical Information Bureau, an association of insurance companies, allows its members to exchange medical information about individuals for, among other purposes, "risk management."[53]

So how does all this occur? A business may create an electronic record of a sale, loan, payment, or other event. Businesses warehouse their own data for their own purposes. Stores may keep track of purchases to understand consumer preference, to track consumer returns, or to predict consumer behavior. For example, Amazon uses existing purchase information to make suggestions to customers.[54] Wal-Mart uses point-of-sale transaction information and warehouses it to identify merchandising opportunities and to manage store inventory.[55] Financial institutions that participate in the Automated Clearinghouse keep records of the electronic payments that consumers make to buy all these goods and services.[56] Any of these businesses may then provide their records of transactions to a data aggregator.

---

[49] *Grocery Store Loyalty Card Use Is Strong Despite Privacy Concerns*, http://i-newswire.com/pr1371.html (last visited Jan. 13, 2007). One study of 515 adults by Boston University's School of Communications found that 86% of adults have at least one grocery store card, and three-quarters of them use a card nearly every time they shop. *Id.*

[50] *See, e.g.*, Catalina Marketing, http://www.catalinamarketing.com/our_advantage/index.html (last visited Jan. 13, 2007). For example, Catalina Marketing claims it logs over a quarter of 1 billion transactions per week from 21,000 supermarkets, tracking the buying behavior of over 100 million households. *Id.*

[51] *See* SOLOVE, THE DIGITAL PERSON, *supra* note 21, at 1.

[52] Frank Main, *Your Phone Records Are for Sale*, CHI. SUN TIMES, Jan. 5, 2006.

[53] Medical Information Bureau, http://www.mib.com (last visited Jan. 13, 2007). This Boston-based company provides information to about 600 life insurance companies, many of which offer other types of insurance for which individuals' histories impact risk, such as health or disability insurance. *Id.* Member companies report medical information to the MIB to be shared with other members. *Id.*

[54] Amazon, www.amazon.com/gp/yourstore/ref+sv_1/002-8216248-8062414 (last visited Jan. 13, 2007).

[55] Walmart, http://www.walmartfacts.com (last visited Jan. 13, 2007).

[56] NACHA, http://www.nacha.org/About/default.htm (last visited Jan. 13, 2007).

With this information, an aggregator's subscriber can decide whether it wants to extend credit to that same individual. Or perhaps the individual already has an account with the subscriber; the subscriber may be seeking an opportunity to raise the rate of an individual cardholder, and can only do so by learning that the same individual has paid another account late.[57] The data created and collected by businesses has significant value to those who would like to identify future customers and political candidates who would like to identify support.[58] Even, and perhaps more disturbingly, governmental agencies have sought access to Americans' transactional biographies.[59]

As a result, a major problem arises when the transactions are mismatched and individuals' images projected from all this digital data distort, leading to a virtual person whose reputation will be tied to the individual despite the mismatch.

C. The Polluted Information Sea

Individuals transact, businesses record those transactions, and aggregators collect those records, connecting the transactions and their details to the individuals to create digital biographies that they and others can mine. However, careless use of information technology has led to aggregators ascribing significant events to the wrong persons. A certain amount of information attributed to any one individual may be false. As businesses, governmental units, and others store more data and increase access to that data, they will also store more inaccurate data and increase the risk that others, including data warehousers, will have access to it and further publish and disseminate it. At the speed of light, the misinformation can spread to a wealth of interested watchers.

Empirical evidence indicates that mismatching leads to inaccurate biographies alarmingly often, whether through undermatching or fuzzy matching. According to the Federal Reserve Board, many consumer

---

[57] *See* Patrick McGeehan, *Soaring Interest Compounds Credit Card Woes for Millions*, N.Y. TIMES, Nov. 21, 2004. Such a provision is called a "universal default clause," and imposes a penalty rate when a consumer pays late to *another* creditor. *Id.*

[58] *See* Kintera, http://www.kinterainc.com/site/C.OWL8JO07KZE/b.1485573/k.BE48/Home.htm (last visited Jan. 13, 2007). For example, Kintera, a software application service provider that supports non-profit organizations, advertises a software product called the Kintera Sphere that can be used by campaigns, fundraising organizations, and other groups to identify potential donors.

[59] Chris J. Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 598, 611 (2004).

credit files contain incomplete or ambiguous information.[60] One study found that almost half of consumer reporting complaints to the Federal Trade Commission ("FTC") involved mismerged files. In nearly two-thirds of those complaints, the consumer's information had been mixed with that of total strangers; in the remainder, the mismatched information belonged to relatives or former spouses.[61] Another study found that nearly 80% of the reports examined contained mistakes of some kind, and a full quarter of the reports contained errors sufficiently serious to cause credit to be denied.[62] Individuals who have purchased their own reports from ChoicePoint, a major data aggregator, have found errors of attribution ranging in import from the relatively minor, such as ownership of autos never owned, to major, such as the individual's own death.[63]

Information attributed to any one particular individual can be false in different ways. The type of falsity addressed here arises when a particular event may in fact have occurred, but the event is treated as the deed not of the originating individual—for example, the person who in fact bought an item, took out a loan, missed a payment—but rather of someone else. Misidentifications that hurt the target's reputation defame. While such misidentifications occurred before the modern information age, the rise of electronic records and their use by the consumer data industry has magnified the impact of this problem.[64]

---

60 Avery et al., *supra* note 45, at 70-71.

61 U.S. PUB. INTEREST RESEARCH GROUP, CREDIT BUREAUS: PUBLIC ENEMY #1 AT THE FTC (Oct. 1993) (on file with author) (analyzing 140 complaints to the FTC). The Fair and Accurate Credit Transactions Act of 2003, required the FTC to report to Congress about the problems of mismerged files. Pub. L. No. 108-159 § 318 (Dec. 4, 2003). The report made a surface evaluation of the costs and benefits of requiring the three largest consumer reporting agencies, Experian, Trans Union, and Equifax, to match more points of identification, and concluded that requiring more matching would reduce mismerged files, and noted that mismerged files "are costly for consumers," but nonetheless emphasized that stricter matching might lead to incomplete files which would decrease their value for users. FEDERAL TRADE COMMISSION, REPORT TO CONGRESS UNDER SECTIONS 318 AND 319 OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 (Dec. 2004), *available at* http://www.ftc.gov/reports/facta/041209factarpt.pdf. The agency did not explain why mismerged files do not similarly impact uncertainty. *Id.*

62 ALISON CASSIDY & EDMUND MIERZWINSKI, MISTAKES DO HAPPEN: A LOOK AT ERRORS IN CONSUMER CREDIT REPORTS 11, 13 (June 2004), *available at* http://www.uspirg.org/uploads/BE/ev/BEevuv19a3KzsATRbZMZlw/MistakesDoHappen2004.pdf [hereinafter MISTAKES DO HAPPEN].

63 Bob Sullivan, *ChoicePoint Files Found Riddled with Errors* (Mar. 8, 2005), http://www.msnbc.msn.com/id/7118767/.

64 *See, e.g.*, Hood v. Dun & Bradstreet, Inc., 486 F.2d 25, 27 (5th Cir. 1973) (misidentifying plaintiff as defendant in two lawsuits when in fact those suits were filed against another individual with the same first and last name).

Some errors occur because the identifying information of the actor is mistranscribed, others because otherwise accurate information is mismatched to the wrong person.

1. Misattribution by Mistranscription

Misattribution may arise when a direct party to a transaction mistranscribes the individual's identifying information.[65] That is, where a party memorializes some sort of financial event, the person or device recording it may fail to assign the event to the identity of its doer, but rather may attach it to the identity of someone else, or even of no one at all. Such misidentification is routinely a matter of human error. A clerk, for example, may mistype a social security number.[66] One jobseeker lost many employment opportunities, learning too late that a sheriff office employee mistyped the social security number of a criminal, substituting the jobseeker's social security number.[67] Alternatively, a machine may malfunction. A fictional, and highly visual, variation of this arises in the film *Brazil*, where a fly falls into a government office's printer, causing the machine to type a "B" in place of a "T" in the name of a man sought by officials. The shift of that one letter sends a swat team to storm into the house of the wrong man as he slept, arresting him in front of his horrified family, and dragging him away. In a real life example, a consumer sued two consumer reporting agencies after they reported that he was a judgment debtor in an amount of nearly half a million dollars.[68] A county clerk had erroneously recorded the judgment in the docket book; in fact, the consumer was the plaintiff in the action, the judgment *creditor*, not the *defendant*; the result was a swing of nearly a million dollars in the plaintiff's favor.[69] However, even though the clerk corrected the information, the two agencies did not pick up the correction and accordingly misattributed the debt to the consumer in a report issued more than six months later.[70]

---

65 *See infra* notes 66-72.

66 Christopher Conkey, *US Gives Some Fraud Victims New Social Security Numbers* (July 6, 2005), *available at* http://www.post-gazette.com/pg/05187/533663.stm (describing case of jobseeker who learned too late that a sheriff's clerk had mistyped his social security number as the number of a convicted criminal).

67 *Id.*

68 Frost v. Experian, No. 98-CIV-2106-JGK-JCP, 1999 WL 287373 (S.D.N.Y. May 6, 1999).

69 *Id.* at *7.

70 *Id.* The court refused the agencies' motion for summary judgment on the plaintiff's claim that the defendants acted willfully, justifying punitive damages under the FCRA. *Id.* at 8; *see also* Henson v. CSC Credit Servs., 29 F.3d 280, 282-83 (7th Cir. 1994) (where clerk

In an infamous instance of misattribution by mistranscription, the consumer reporting agency TRW, Experian's predecessor, contracted with an outside company to review a Vermont town's public records to find those consumers who had defaulted on their property taxes.[71] The researcher copied information from the wrong rolls, and as a result, all compliant property owners in the town were reported as delinquent in paying their property taxes.[72]

In contrast to these ordinary misattributions, sometimes misidentified information arises when a third party, an identity thief, intentionally misdirects the recorder into mistranscribing the victim's identifying information as the thief's, pinning the wrong identity to the act. This crime has received marquee attention of late:[73] with the rise of instant credit, electronic transactions, and easy access to personal identification keys such as social security numbers and account numbers, identity theft has soared.[74] Both federal and state laws now specifically criminalize it.[75] But identity theft is not new—impostors have likely been with us since sufficient people inhabited the earth to support it.[76] Nonetheless, the crime is much easier now that disconnected transactions have supplanted so many face-to-face ones.

In a typical identity theft case, the thief uses a consumer's identifying information to create new accounts with merchants, creditors, and other

---

mistakenly recorded a judgment in a suit brought against two brothers in both their names when judgment was in fact against only one).

71 Sharon Kindel, *Garbage In: Credit Bureaus Have Terrible Error Rates*, FIN. WORLD, Sept. 29, 1992, at 61.

72 *Id.*

73 Federal Trade Commission, http://www.ftc.gov/opa/2005/02/top102005.htm (last visited Jan. 13, 2007). For example, identity theft has been the subject of the most complaints to the FTC every year since 2000. *Id.* The FTC has developed a sizable set of web materials. *See* Federal Trade Commission, *Fighting Back Against Identity Theft*, http://www.consumer.gov/idtheft/ (last visited Jan. 13, 2007).

74 FEDERAL TRADE COMMISSION, IDENTITY THEFT VICTIM COMPLAINT DATA: FIGURES AND TRENDS, JANUARY 1-DECEMBER 31, 2005, http://www.consumer.gov/idtheft/pdf/clearing house_2005.pdf. Identity theft accounted for more than 255,000 complaints to the FTC's fraud and identity theft complaint database, Consumer Sentinel, in 2005. *Id.* The complaints had increased by about 9000 from 2004. *Id.*

75 *See, e.g.*, The Identity Theft and Assumption Deterrence Act, 18 U.S.C. §§ 928(b)(1), 1028 (2000); CAL. PENAL CODE §§ 530.5-530.8 (West 2006); N.Y. PENAL LAW §§ 190.77-190.84 (McKinney 2005); TEX. PENAL CODE ANN. § 32.51 (Vernon 2003).

76 HERODOTUS, THE HISTORY bk. 3, at 61 (David Grene trans., Univ. of Chi. Press 1987). As just one example, in ancient Persia, a Magian impostor adopted the identity of Smerdis, King of Persia (and the second son of Cyrus the Great), after Smerdis was assassinated. *Id.* The false Smerdis was overthrown and slain in 521 B.C., after reigning for seven months. *Id.* at 79.

third parties, then uses those accounts to acquire goods and services for which the thief will not pay.[77] The misattribution arises when the business entity ties the transaction to the victim's identity markers instead of the thief's. After failing to obtain the correct identifying information, the entity assigns the transaction to the wrong person. Eventually, the recording entity will report the transaction to a data aggregator, such as a consumer reporting agency, as being the victim's work, rather than the thief's.

Public records become polluted by mistranscription as well. For example, an identity thief may commit a crime in the name of another and, upon arrest, give the arresting officer the identifying information of the victim. The jurisdiction of the arrest will dutifully record that information in a computer—thus further victimizing the original victim—and treat it as if the information were verified. If we assume that the thief in fact committed the underlying crime, the falseness in the new information lies not in the fact of the event having occurred—the assault, the burglary, the drug use—but in the identity of the actor in the event. Someone committed the act, but not the person the database now records as having done so.

Civil public records have also become tainted. Although less serious than a wrongful conviction, identity thefts in bankruptcy courts have been rising, leading some individuals to have to fight to have a bankruptcy they never filed removed from their name.[78] In this case, it is the court clerk who misattributes the events to the victim, having failed to verify the filer's identity.

From one standpoint, the cause of this misattribution is the thief's use of the identifying information of another. However, from another, the cause of this misattribution is the failure of the recorder, business, or public entity to do as much as it could to verify the identity of those with whom they deal. The significant damage that thieves do to individuals arises not from the work of the impostor, but from the responses of others. It is not the thief who records the account, the creditor does that. It is not the thief who reports the new debt in the victim's name, the creditor does that as well, and the aggregator, not the thief, falsely

---

77 *See Fighting Back Against Identity Theft*, *supra* note 73; Privacy Rights Clearinghouse, *Coping with Identity Theft: Reducing the Risk of Fraud*, http://www.privacyrights.org/fs/fs17-it.htm#crime (last visited Jan. 13, 2007) (This sort of identity theft is also known as "'true name fraud.'").

78 Peter C. Alexander, *Identity Theft & Bankruptcy Expungement*, 77 AM. BANKER L.J. 409, 411-12 (2003).

reports to others that the debt is the victim's, rather than the thief's. In this way, the damage done to a reputation by identity theft differs little from that caused by non-criminal carelessness. For purposes of record matching, the intent of the actor matters less than the actions of the person or entity that tags the thief's acts with the victim's identity markers. The injury suffered by identity theft victims would not arise without the participation of the third parties in the data market.

Thus, although motivations behind mistranscription errors vary, the common underlying element is the creation of a record that describes an event that actually occurred, but ascribes it to the wrong person. The event then pollutes the transactional biography of the misidentified doer, corrupting the image that the biography portrays to the world, and thus deflating (if negative) the degree of esteem the doer has earned.

2. Misattribution by Mismatching

Mistranscription is one form of mismatching but a more pervasive problem of misattribution arises where the identity information of a particular record of an event is mismatched to the identity of someone with superficially similar identifying information. The three major consumer data aggregators, Experian, Trans Union, and Equifax (also known as consumer reporting agencies), do not simply add each new record to a consumer's file the way, for instance, a lawyer would keep a file for a client and add to it letters from that client, pleadings from the client's case, and such.[79] Rather, data providers, such as merchants and creditors, send records to the agencies with the identity markers of the individual to whom the provider attributes the event, such as name, date of birth, and social security number, and the agencies store the records in their databases.[80] When an agency's subscriber seeks a report about a particular individual, the subscriber supplies identifying markers (or pegs, in Goffman's terms) and, applying this identifying information, the agency's computer runs an algorithm that searches the databases for records with matching, or similar, identifying information.[81] Thus, the file is pulled together dynamically at that moment for the immediate purpose.[82] The matching algorithm, rather than the record's location,

---

79 HENDRICKS, *supra* note 39, at 144.

80 *Id.*; *see also* Sarver v. Experian Info. Solutions, 390 F.3d 969, 972 (7th Cir. 2004).

81 HENDRICKS, *supra* note 39, at 144; *see also Sarver*, 390 F.3d at 972 (describing process); Apodaca v. Discover Fin. Servs., 417 F. Supp. 2d 1220, 1224 (D.N.M. 2006) (same); McKeown v. Sears Roebuck Co., 335 F. Supp. 2d 917, 930-31 (W.D. Wis. 2004) (same).

82 *See Apodaca*, 417 F. Supp. at 1224 (describing process); *McKeown*, 335 F. Supp. 2d at 930-31 (describing process).

determines whether the record of a particular event will be assigned to the specific individual or not.[83] The algorithm determines both the identity markers that it will examine and the degree of fuzziness it will tolerate in matching those markers. For example, the algorithm of one major agency, Experian, uses thirteen matching elements, including not just a full social security number, but also a mere fragment.[84] Misattribution by mismatching may arise through undermatching or fuzzy matching.

a. Undermatching

Undermatching can arise when the identifying information attached to a particular event is insufficiently complete to avoid ambiguity.[85] For example, an event may be identified by only a person's name. As an example of this sort of misattribution, a doctor's office clerk may put the test results of one James Jones into the file, whether paper or electronic, of another James Jones. Although other markers of the two individuals' identities, such as middle name, date of birth, place of birth, and telephone number, may be different, the data is "undermatched"—limited to the first and last names when more identifying information is necessary to match the record to a single individual.

In the doctor's office example, the creator of the record misidentifies the actor if she selects the wrong James Jones. However, misattribution by undermatching also arises when the record is collected by a data aggregator that then uses the imprecise identifying information to misattribute the act to another. This sort of misattribution, also known as mismerging, is often to blame for bad transactional biographies.[86] In mismerging, a data aggregator incorrectly identifies a particular event as being the responsibility of the targeted individual. In contrast to misattribution by mistranscription, where the error arises at the initial recording of the data, misattribution by mismatching arises when a party tries to match a particular record to the identity of someone already

---

[83] HENDRICKS, *supra* note 39, at 145-47.

[84] *Id.* at 146. The agency's algorithm also uses the following elements: last name; first name; middle name; suffix; age; gender; street number; street name; apartment number; city, state, and zip code; and trade account number. *Id.*

[85] This concept is also sometimes referred to as "partial matching." *See, e.g.*, *Apodaca*, 417 F. Supp. at 1224 (describing logic); HENDRICKS, *supra* note 39, at 148-51.

[86] CONSUMER FEDERATION OF AM. AND NAT'L CREDIT REPORTING ASS'N, CREDIT SCORE ACCURACY AND IMPLICATIONS FOR CONSUMERS 35 (Dec. 17, 2002), *available at* http://www.consumerfed.org/121702CFA_NCRA_Credit_Score_Report_Final.pdf [hereinafter CREDIT SCORE ACCURACY]. Nicknames, misspellings, transposed social security numbers, and mismatching all contribute to merging errors. *Id.*

known. The mismatching arises when a data aggregator chooses to undermatch the record to an individual on the basis of some identity markers.

As an example of incomplete identifying information, a record may identify a transaction as belonging to a John Q. Public, and in fact the aggregator has records belonging to more than one—perhaps several—John Q. Publics lurking within the depths of its databases. The aggregator may assign the record to all of them when it goes fishing for a specific John Q. Public's file, which is not a problem, necessarily, if it ends up on the record of the John Q. Public who incurred the transaction, but potentially quite a problem if it ends up on the record of a John Q. Public who did not. For example, in *Apodaca v. Discover Financial Services*,[87] a consumer named Victoria Apodaca spent nearly a year trying to disconnect the bankruptcy and debts of another woman, Victoria Lopez Apodaca, from her credit report.[88] The aggregator does not intend to tie the fact of the event to the wrong individual, the wrong construction of Locke's "organized Body," but it does so anyway because it did not sufficiently identify the person on whose identity peg the event should be hung. Such a mistake may be the result of an identity thief seeking to intentionally mislead a creditor or a consumer reporting agency into misreporting a transaction as having been incurred by the robbed. Such a thief may have some, but not all, of the usual identity markers of the victim.

Data aggregators are motivated to match each transaction that comes in to a particular consumer. These transactions only have value to the aggregators' subscribers who purchase the information if they are attributed to a particular individual. Data aggregators' customers do not subscribe to them to find out if a particular event occurred—that is, to find out whether someone, anyone, owes $5,000 to Sears, $3,000 of which comprises late fees and accumulated interest. No, what subscribers to the credit reporting agencies and other data aggregators want to know is *who* bought what, *who* incurred that debt, *who* is responsible for repaying it. The information of the transaction alone is not what makes the information valuable. It is the matching of the transactions with the individual—the connecting piece—that makes the information valuable. This motivation can raise the risk of mistattribution.

---

87 417 F. Supp. 2d 1220.

88 *Id.* at 1222-25. Seven of nine digits in the two women's social security numbers matched, but they lived in different towns and shared no other identifying markers. *Id.* at 1224.

The most routine sort of undermatching is matching on the basis of name alone. However, as Erving Goffman has pointed out, the personal name as an identity marker, while the most commonly used, is at the same time far from the most reliable.[89] The doubt is particularly high with relatively common names. Undermatching has been visible lately in the mishaps of the Transportation Security Administration's "No Fly" List, where travelers unfortunate enough to have a name the same as or similar to that of a suspected terrorist target are pulled aside for questioning.[90] Similarly, in the 2000 election, some Florida voters were turned away from the polls as being ineligible to vote based simply on the match of their names to names on a list of convicted felons pulled together by a data aggregator.[91] The rise in the sheer number of American consumers indicates that relying merely on personal names to tie an event to an individual is increasingly risky, at least where the event is disconnected from that individual so that no party to the transaction is familiar with any other. Given that more than 2.9 million individuals reside in the United States, the chances that many of them will have duplicate names appear to be quite high.[92] Thus, matching by name alone appears foolishly to invite misattribution.

Additionally, undermatching is often to blame when an aggregator poisons an individual's financial transaction biography with an identity thief's transactions. A data provider will report an account using the identifying information provided by the thief. While often the name and social security number attached to the thief's transaction will match those on the victim's biography, nonetheless other identity pegs provided by a thief that would pinpoint identity, such as date of birth, place of birth, address, and telephone number, will conflict with those in

---

89 GOFFMAN, *supra* note 1, at 58*; see also* CECIL ROLPH, PERSONAL IDENTITY (1957).

90 Complaint, Green v. Transp. Sec. Admin. (W.D. Wash. 2005) No. CV04-0763. The ACLU has filed a class action complaint against the Transportation Security Administration, among others, alleging that hundreds of innocent travelers have been detained because they have names similar or identical to those on the "No Fly" list, notwithstanding that they have no ties to terrorist activities. *Id.* According to the ACLU's complaint, the No-Fly List includes additional identity markers for its members, including date of birth, nationalities, and passport numbers, but the list nonetheless is incomplete and inaccurate. *Id.* ¶ 20.

91 Robert E. Pierre, *Botched Name Purge Denied Some the Right to Vote*, WASH. POST, May 31, 2001, at A01. The aggregator, DBT Technologies, has since been acquired by ChoicePoint. *Id.*

92 State and County Quickfacts, http://quickfacts.census.gov/qfd/states/00000.html (last visited Jan. 13, 2007). The United States Census Bureau estimates that the number of people in the United States in 2005 was 296,410,404—an increase of 5.3% from 2000. *Id.*

the aggregator's database.[93] When the aggregator runs its matching algorithm through its warehouse, the algorithm pulls up the fraudulent accounts, matching only an inadequate number of identity markers while disregarding additional identity markers that conflict with the victim's information.[94]

The advances in data technology have contributed to errors by undermatching. The risk of undermatching arises not just because so many people have the same name as someone else, but because the pool of collected data has grown so large. A data aggregator that culled only data from one particular area, geographic or demographic, would run a lower risk of collecting records that bear the same name, but nevertheless refer to two (or even more) different individuals.

Furthermore, undermatching increases when we disaggregate the doer from the deed. The record, once it leaves the context of the original event, becomes skinned of the additional identifying attributes that context provides. For example, the record of a James Jones in a certain doctor's office will be identified by the other identity markers the office may use that do not become part of the record. The office staff may be perfectly able to keep their two James Joneses apart, whether because of office filing practices or because they suffer from different ailments or because of some other distinction. But once the record leaves that context, it loses those markers and must compete with other records of other James Joneses.

b. Fuzzy matching

The second main type of mismatched transactional information arises not from undermatching, but from fuzzy matching.[95] Fuzzy matching imposes vagueness on identity markers, blurring precision. Vagueness can be imposed at the level of a given individual marker, for example, where the name James Jones is deemed to match Jim Jones and Jimmy Jones. The vagueness can also be imposed at the next level up, where multiple markers are matched. For instance, a record will be matched to a person if the name and the city of residence match, even if

---

93 *See* Wade v. Equifax, No. 02-C-3205, 2003 WL 22089694, at *4 (N.D. Ill. Sept. 8, 2003) (where provider who had reported an account opened by an identity thief as being the plaintiff's, even though the plaintiff's name, Lori Wade, differed substantially from the name the thief used, Lori White).

94 *See, e.g.*, Dornhecker v. Ameritech Corp., 99 F. Supp. 2d 918, 922 (N.D. Ill. 2000).

95 *See* THE NEW SHORTER OXFORD ENGLISH DICTIONARY ON HISTORICAL PRINCIPLES 1048 (1993) (noting that in computing and logic usage, "fuzzy" can be "defined so as to allow for imprecise set-membership").

other markers, such as date of birth, do not. So, for example, one data aggregator, a consumer reporting agency, misattributed a bankruptcy of a "Donela Reed" to her brother "Donel."[96] In addition to similar names, the siblings had similar social security numbers; nonetheless, the names, social security numbers, and, obviously, genders of the two individuals were distinctly different.[97] The fuzziness calls a match even though the two sets of identity markers, while overlapping, do not match entirely. For example, the aggregator may identify a record to an individual with a similar, yet distinctly different, last name if the first names match.[98] Aggregators' algorithms, which search through the data warehouse for records with similar, but not identical, identifying information use fuzzy matching to collect transactional biographies.[99]

Fuzziness will often poison the data sea by falsely attributing one person's action to another. However, some fuzziness may lead to accurate attribution, which is why data aggregators employ it. An accurate reputation may in fact depend on imprecise or unverifiable information. As Samuel Johnson once said, "If a man could say nothing against a character but what he can prove, history could not be written."[100] If the only transactions that could be ascribed to an individual were those for which the doer's identity had been fully verified, many who depend on aggregators' reports to accurately portray the image of the individual would be misled. For example, a James Jones may in fact have signed his name as Jim, and to reject that record on the basis of the mismatch in first names would lead to a financial biography for James Jones that portrays a truncated image, leading to an inaccurate reputation. Nonetheless, errors from fuzzy matching could be minimized by verifying the match of additional markers that are unlikely to vary, such as the date or place of birth.

D. Inaccuracies in the Data Warehouses

Not all misattributions of transactions lead to litigation, but those that do indicate that mismatching errors are hardly unavoidable. An aggregator may match records even when the names have only a passing resemblance. For example, one data aggregator attributed the account of

---

96 Reed v. Experian Info. Solutions, Inc., 321 F. Supp. 2d 1109, 1111-12 (D. Minn. 2004).

97 *Id.*

98 *See, e.g.*, McKeown v. Sears Roebuck & Co., 335 F. Supp. 2d 917, 925-26 (W.D. Wis. 2004) (agency matched record of the death of an individual named McOwen to the plaintiff, notwithstanding the difference in names).

99 *See supra* text accompanying notes 93-94.

100 JAMES BOSWELL, LIFE OF JOHNSON 727 (1998).

an identity thief who had used the name "Lori White" to someone named "Lori Wade."[101] Similarly, in *McKeown v. Sears*, a consumer reporting agency attributed the account of a James N. McOwen to the plaintiff, James McKeown.[102] The plaintiff learned of the misattribution when he tried to apply for credit, and an agency issued a credit report for him indicating that he was dead.[103] The error arose because Sears had noted in its own files that an account holder named James N. McOwen had died, but the note lacked additional identity markers, raising a real risk of undermatching.[104] Later, Sears matched the report of death with the plaintiff's account number, apparently by fuzzily, very fuzzily, matching the record by name to the plaintiff, even though the two had different middle initials, different numbers of letters in their last names, and different arrangements of those letters.[105] Two consumer reporting agencies then published the deceased notation.[106] Thus, through a combination of fuzzy matching and undermatching, the plaintiff was reputed to be dead.

Even matching first names and last names can lead an aggregator to wrongfully ascribe one individual's act to another. For example, in *Jones v. Credit Bureau of Great Garden City, Inc.*,[107] the defendant, a consumer reporting agency, had ascribed to a "James R. Jones" the debt of a "James D. Jones."[108] The agency made this match notwithstanding that the two individuals had different middle initials, different addresses, and different dates of birth.[109] Even if such fuzzy matching were an appropriate way to ascribe information in the case of a rare surname, it seems downright rash in the case of a last name such as "Jones," especially when combined with a relatively common first name. The court agreed, finding that the consumer reporting agency could be negligent for failing to verify the identity of the debtor.[110] In a similar

---

101 Wade v. Equifax, No. 02-C-3205, 2003 WL 22089694, at *4 (N.D. Ill. Sept. 8, 2003).

102 *McKeown*, 335 F. Supp. 2d at 925-26.

103 *Id.* at 925. The court denied the motion of a consumer reporting agency, Trans Union, to dismiss the plaintiff's claim under the FCRA. *Id.* at 925-26, 935. In response to the plaintiff's dispute, the agency reaffirmed the validity of the match. *Id.* Even though Sears reaffirmed the identity of the account, it noted that the name on the account differed from the one the agency provided with the dispute. *Id.*

104 *Id.* at 924.

105 *Id.*

106 *Id.*

107 No. 87-1302-C, 1989 WL 107747 (D. Kan. Aug. 29, 1989).

108 *Id.* at **3-4.

109 *Id.*

110 *Id.* at *7. The injured debtor and his wife brought a claim pursuant to the FCRA. *Id.* The court was unimpressed with the agency's matching techniques: "Defendants' transfer of information from one debtor's credit file into another debtor's credit file is undoubtedly

fashion, a consumer reporting agency mixed together the financial events of a "William Daniel Thompson, Jr." and "William Douglas Thompson, III," notwithstanding that the records' identifying information included different social security numbers, different addresses, and different occupations.[111]

Some aggregators' fuzzy matching policies seem nearly designed to create false biographies. For example, one agency has used an algorithm that attributes a record to an individual if *any* two of the identity markers matches, yet deems the name marker matched if the main name, without any suffix such as "junior," matches.[112] Furthermore, the agency may verify the match even after a misidentified individual challenges it.[113] This, predictably, will create false virtual images whenever a father and an adult son named after him live at the same address. The image portrayed by the aggregator's report will be a mish-mash of the two, the reputation true to neither.

Fuzzy matching of public records can also lead an aggregator to falsely report that one individual's bankruptcy was filed by another. A consumer reporting agency reported one woman's bankruptcy in the name of another woman who lived in a different town, was born on a different day, and had a different middle name and a different social security number.[114] In another case of false attribution of bankruptcy, a mortgagee reported that the bankruptcy of one co-obligor on a mortgage was in fact that of the other, notwithstanding that the two had dissimilar names and that the non-bankrupt borrower had continued to pay the debt.[115]

---

a serious and significant act which calls for more precautions than a similarity of names." *Id.*; *see also* Apodaca v. Discover Fin. Servs., 417 F. Supp. 2d 1220, 1224 (D.N.M. 2006) (denying agency's motion for summary judgment where two women shared the same name and seven digits of their social security numbers but nothing else).

111 Thompson v. San Antonio Retail Merchs. Ass'n, 682 F.2d 509, 513 (5th Cir. 1982) (affirming lower court's judgment that a consumer reporting agency's verification process that did not require sufficient "points of correspondence" between the consumer and the file or did not have an adequate auditing procedure to foster accuracy, violated the FCRA).

112 Moore v. Equifax Info. Servs. L.L.C., 333 F. Supp. 2d 1360, 1365 (N.D. Ga. 2004) (denying agency's motion for summary judgment on claim brought pursuant to 15 U.S.C. §§ 1681e, 1681i (2000)).

113 *Id.*

114 Kenneth R. Gosslein & Matthew Kauffman, *A Credit Trap for Consumers*, HARTFORD COURANT, May 26, 2003, at A1.

115 Nelson v. Chase Manhattan Mortg. Corp., 282 F.3d 1057, 1058 (9th Cir. 2002).

Additionally, criminal record information can be particularly damaging, yet is also especially subject to mismatching errors.[116] In fact, the poor quality of compiled "[r]ap sheets" was one reason the Supreme Court upheld the denial of a Freedom of Information Act request to obtain such documents from the Federal Bureau of Investigation in *United States Department of Justice v. Reporters Committee for Freedom of Press*.[117] Justice Stevens, writing for the Court, blamed the poor quality of the sheets on the amount of information: "Because of the volume of rap sheets, they are sometimes incorrect or incomplete and sometimes contain information about other persons with similar names."[118] That was in 1989; since then, the volume of personally identifiable information has grown tremendously.

Not just individuals have data mismatched; businesses can suffer from undermatching and fuzzy matching as well. In one commercial defamation case, the plaintiff, County Vanlines, Inc., sued a consumer reporting agency for defamation after it was denied a loan because the agency had sent the intended lender information about negative credit events that were incurred by a business with the similar but, nonetheless, distinctly different name of County Van and Storage, Inc.[119] The agency did so notwithstanding that the transactions took place before the target moving company had even incorporated.[120] The defendant justified the loosely-matching algorithm on the grounds that precision would eliminate accurate and relevant data.[121]

These cases indicate that some credit reporting agencies do relatively little meaningful matching of the data already in their data warehouses

---

116 *See, e.g.*, Dalton v. Capital Associated Indus., Inc., 257 F.3d 409, 412-14 (4th Cir. 2001). The plaintiff had applied for a job and had truthfully represented on the application that he had not been convicted of a felony, although he had been convicted of a misdemeanor. *Id.* at 417. The investigating agency uncovered the misdemeanor as part of the background check, but misreported it as a felony based on the erroneous opinion of the county clerk, which the agency did not verify. *Id.* The court of appeals vacated summary judgment, which was favorable to the agency, based on a factual dispute raised by the plaintiff's claim that the agency had violated the FCRA by failing to use reasonable procedures to assure the maximum possible accuracy of the information in the plaintiff's report. *Id.*

117 489 U.S. 749, 752 (1989). The Court held that the FBI could deny access to the rap sheets pursuant to 5 U.S.C. § 552(b)(7)(C), which allows an agency to deny a FOIA request for "law enforcement records or information about a private citizen" if disclosure could "reasonably be expected to invade that citizen's privacy." *Id.* at 780.

118 *Id.* at 752.

119 County Vanlines, Inc. v. Experian Info. Solutions, Inc., 317 F. Supp. 2d 383, 385-86 (S.D.N.Y. 2004).

120 *Id.* at 386.

121 *Id.* at 388-89 (reciting testimony of the technical manager of the defendant).

before attributing events to a particular individual, leading to the high risk that the individual was not in fact the person who participated in that event.

E. The Power of Bad Data

In sum, advances in information technology have led to businesses, creditors, and others storing digital records of consumers' financial transactions. Technology has helped speed the duplication and distribution of these sorts of records. Data aggregators can then warehouse and analyze them, both for the benefit of those with which an individual currently does business and for those that would like to find new individuals with whom to do business. In this way, transactional biographies develop, creating a virtual image. However, errors abound in the sea of data, a "frothy Chaos" of undermatched and fuzzily matched information that taints people's biographies with gossip and rumors.[122] Accordingly, the image that observers treat as though it faithfully represents someone may not in fact do so. However, how important are these errors? What impact can a false biography have on individuals and on society at large? How does such digitized information have more power than its print version? As discussed below, it has so much power that it can effectively shut a consumer out of the opportunity to enter into new transactions.

The same characteristics of digitized, networked data that give it so much power pertain to that data even when it is false. While information about individuals has never been perfectly accurate, inaccurate data has more impact now than ever for the same reasons that accurate data does.[123] First, data is much more accessible than it used to be. Accordingly, what errors might have been seen by just a few viewers—albeit viewers who could possibly have great power over the subject of that news (as one imagines William the Conqueror had)—can now be released onto the Worldwide Web and accessed anywhere by anyone with an Internet connection. Furthermore, the information age has detached data from the original actor and from the transaction that created it, which means that the observer of the electronic record may never perceive any supplemental information that could correct or ameliorate misattributed information held in a physical record. Because the data and its creators, storers, and users are often so detached from the person to whom it pertains, it may be far more difficult for an

---

122 Montaigne, *supra* note 2.

123 *See infra* text accompanying notes 131-33.

individual to correct it. A false report of someone's death in a small community, for example, could be easily remedied simply by the alive-and-well person appearing, in the flesh, before the person who started the rumor. If the data were in a paper record, that record could be corrected. The person could similarly appear before those who had been falsely told (or had read) of the death. The chances that the original record had been copied many times were likely small and, by correcting the original, the individual could be reasonably sure that any copies in the future would omit the inaccurate item. Now, however, an individual may learn of a false attribution only after the record has been copied and distributed far and wide and, even if able to correct it at the original source, may have no ability to retrieve all the bad copies.

Face-to-face transactions have yielded to the convenience and efficiency of electronic ones, and information generated from those transactions gains impact because it is much less likely to be paired with or ameliorated by first-hand impressions. For example, a mortgage decision might well come down to a simple credit score,[124] a number sprung from information, whether accurate or not, linked to one's credit history, without the lender ever meeting the applicant face-to-face.[125] Even if the borrower actually meets with a lender's representative, that representative will likely rely on reports generated not from (or at least

---

124 *See infra* text accompanying note 134.

125 The 2003 revisions to the FCRA define a credit score as follows:

> (i) . . . a numerical value or a categorization derived from a statistical tool or modeling system used by a person who makes or arranges a loan to predict the likelihood of certain credit behaviors, including default (and the numerical value or the categorization derived from such analysis may also be referred to as a "risk predictor" or "risk score"); and
>
> (ii) does not include—
>
> > (I) any mortgage score or rating of an automated underwriting system that considers one or more factors in addition to credit information, including the loan to value ratio, the amount of down payment, or the financial assets of a consumer; or
> >
> > (II) any other elements of the underwriting process or underwriting decision.

Pub. L. No. 108-159, § 212(b) (2003) (codified at 15 U.S.C. § 1681g(f)(2)(A) (2000)). As amended, the Act requires agencies to disclose credit scores to consumers upon request. Pub. L. No. 108-159, § 212(b) (2003) (codified at 15 U.S.C. § 1681g(f)(1)). Credit scores have even been used by airlines to screen passengers for potential security risks. Donna Havorsen, *For Some, Use of Credit Scores Doesn't Add Up*, STAR TRIB. (Minneapolis-St. Paul), Mar. 13, 2003, at 1A.

not solely from) the lender's own experiences with the borrower, but from those of many others.[126]

Aside from practical damages such as these, however, false attribution of others' deeds damages the dignity of a person as well. Both of these types of damages are discussed below.

1. Tangible Damages to Reputation

The "digital dossier" of our commercial transactions with others has enormous power:[127] it can determine whether and on what terms a person can obtain a credit card, rent an apartment, buy a home, get a particular job, or obtain utility service.[128] The dossier has this power regardless of whether the information within it is true. The creditor, landlord, mortgagor, or business will decide whether to do business with an individual and, if so, the terms of that business, based on the history prepared by the data aggregator, regardless of the accuracy of that reported history.

For our purposes, "reputation" refers to the perception of the community of the construct, the constitutive parts, of the individual.[129] False data that is negative damages that perception by lowering the estimation of the person in the eyes of those that check for worthiness to participate in commercial transactions. Observers identify the image of a person with the person as he or she really is. Accordingly, a reputation arising from the image created by the mis-merged information will nonetheless be treated as true to that individual.

As discussed above, mismatching errors on credit reports are common, and they are far from harmless.[130] The Consumer Federation of America reported in 2002 that errors in consumer credit reports could cost consumers millions of dollars in higher costs for credit.[131] A 2004

---

126 *See also* HENDRICKS, *supra* note 39, at 40-45.

127 *See* SOLOVE, THE DIGITAL PERSON, *supra* note 21, at 1-2, 49.

128 A regulatory agency may allow a utility company to demand a deposit from a residential applicant based on the credit history attributed to an individual. *See, e.g.*, 83 ILL ADMIN. CODE § 280.50(a) (2006) (allowing utility companies to demand a deposit from residential service applicant's whose credit scores fail to meet the service's standards).

129 *See supra* text accompanying notes 15-16.

130 *See supra* text accompanying notes 87-88, 93-98.

131 CREDIT SCORE ACCURACY, *supra* note 86. Of the credit reports reviewed, 29% contained serious errors—false delinquencies or accounts that did not belong to the consumer—that could cause a creditor to deny credit. *Id.* at 6. In 2003, the U.S. General Accounting Office concluded that more study concerning the accuracy of credit reports is needed. U.S. GEN. ACCOUNTING OFFICE, CONSUMER CREDIT: LIMITED INFORMATION EXISTS

study found that one in four of the credit reports reviewed contained errors sufficiently serious to cause a creditor to deny credit; many of these errors were bankruptcies, accounts, and other items that did not belong to the identified individual.[132]

To illustrate the crippling effects that mismatching of electronic data can cause, we will use a fictional individual, Charlie Consumer, who has led a fairly ordinary life, transaction-wise. Somewhere else a Charley Consumer, who has the same last name and a similar first name to our subject's, has lived the life of a deadbeat. The two may live near one another and may even have similar social security numbers. Nonetheless, the two have no other identity markers in common—that is, they have different dates of birth, different places of birth, different (though perhaps similar) social security numbers, and so forth.

Charley-the-scoundrel acquires a credit card from a credit card company and uses it to mount up debts that he failed to pay. The credit card company records the delinquency and reports it, associated with the name, address, date of birth, social security number, and telephone number of the originating Charley, to a consumer reporting agency to which the company subscribes. The agency stores the record in its vast data warehouse, where it stays until called up.

This record, if fuzzily matched to the creditworthy Charlie, can devastate his ability to develop and live his life. It can keep him from buying a house,[133] or perhaps allow him to do so only at a much higher interest rate.[134] In effect, Charlie is charged with being someone who

---

ON THE EXTENT OF CREDIT REPORT ERRORS AND THEIR IMPLICATIONS FOR CONSUMERS 17 (July 31, 2003).

132 CASSIDY & MIERZWINSKI, *supra* note 62, at 6, 11. The study by the Massachusetts Public Interest Research Group in 2004 of 154 consumers and their credit reports found that 79% of the credit reports contained mistakes. *Id*. at 4. One in four contained serious errors that could result in the denial of credit; nearly one in three contained credit accounts listed as open that had been closed by the consumer. *Id*.

133 *See infra* text accompanying note 134.

134 *See* McCloud v. Homeside, 309 F. Supp. 2d 1335, 1338 (N.D. Ala. 2004) (plaintiff whose former mortgage lender wrongfully reported her as delinquent could qualify only for "'sub-prime'" financing at an elevated rate); Graham v. CSC Credit Servs., Inc., 306 F. Supp. 2d 873, 876-77 (D. Minn. 2004) (alleging that an erroneous mismatch led a mortgagee to offer plaintiff an interest rate one half percent higher on a fifteen year loan); McKeown v. Sears Roebuck & Co., 335 F. Supp. 2d 917, 925-926 (W.D. Wis. 2004) (plaintiff who was falsely matched with the record of a dead individual lost the opportunity for a thirty-year fixed mortgage and instead had to take an adjusted rate mortgage with only the first five years fixed); Gordon v. Greenpoint Credit, 266 F. Supp. 2d 1007, 1009 (S.D. Iowa 2003) (erroneous credit report caused two lenders to deny plaintiffs a loan and a third lender to offer a loan at an elevated rate).

largely lived the same life as he did, but who incurred this bad debt. The bank, however, treats the blended image of Charlie and Charley as being a true portrayal of Charlie's transaction history. Charlie's reputation for creditworthiness has suffered from the mismatch of Charley's information to his identity.

If Charlie seeks instead to rent a home, a report containing Charley's bad debt may keep him from being able to do so.[135] It may also prevent him from getting a job.[136] Employers may rescind a job offer, or even fire an employee, if dissatisfied with the individual's financial history.[137] In fact, employers commonly scan this kind of information; according to one survey, more than one-third of employers surveyed used credit reports to screen candidates.[138]

By the time Charlie learns through these denials and rejections that his biography has been contaminated by false information, it may be too late to repair the image that the inaccurate biography projects. For example, one consumer lost his job after a consumer reporting agency incorrectly ascribed a drug conviction to him, when in fact the conviction had been incurred by a man with the same first and last name, but with a different middle name and date of birth.[139] In such cases, the consumer has no right to delay the decision while the record is corrected.

---

135 Motoko Rich, *TURF; A Blacklist for Renters*, N.Y. TIMES, Apr. 8, 2004, at F1 (describing suit brought against tenant screening agency alleging that the company provided incomplete and inaccurate information). Many landlords use tenant screening companies that aggregate information from, among other sources, consumer reporting agencies. *Id.*; *see* Josh Barbanel, *Residential Real Estate; Suit Disputes the Accuracy of Tenant Screening Reports*, N.Y. TIMES, Feb. 27, 2004, at B8 (describing tenants who were unable to rent new apartments because a tenant screening company reported that they had been involved in housing lawsuits, even where suits were resolved in the tenants' favor).

136 *See, e.g.*, Wiggins v. Equifax Servs., Inc., 848 F. Supp. 213, 217 (D.D.C. 1993) (involving suit arising after plaintiff was fired because agency reported felony drug conviction in name of James Ray Wiggins to the plaintiff's identity, James Russell Wiggins, even though their dates of birth differed); *see also supra* text accompanying note 125. Although the FCRA requires employers to obtain a job applicant's consent to the credit search, 15 U.S.C. § 1681b(b)(2)(A) (2000), nothing prevents an employer from conditioning an offer on such consent.

137 *See* HENDRICKS, *supra* note 39, at 4-6.

138 Andrea Coombes, *Job Seeker's Obstacle: Bad Credit* (June 17, 2004), http://www.marketwatch.com/news/story/story.aspx?siteid=mktw&guid=%7B282DE3FC-0D52-4211-AB1F-A07A0A35CEFD%7D. Federal law requires employers to obtain the employee's or applicant's consent, 15 U.S.C. § 1681b(b)(2)(A), but the employer may fire the employee or deny the application if consent is refused. *Id.*

139 Wiggins v. Dist. Cablevision, Inc., 853 F. Supp. 484, 488-89 (D.D.C. 1994) (an example of fuzzy matching); *see also* Nelski v. Ameritech, No. 244644, 2004 WL 1460001, at *1 (Mich. Ct. App. June 29, 2004) (the defendant, a mobile telephone services provider, opened up an

Just as a tainted credit record may deny him the ability to find a place to live or work, it may prevent Charlie from buying or leasing a car.[140] It may prevent him from obtaining additional credit cards. Possibly worse, his existing credit card company could routinely scour the records aggregated at agencies for signs of instability, and use the record of the delinquent account to invoke a universal default clause that allows the card company to raise the interest rate on a charge account that Charlie really does own, a financial consequence that could in fact cause the very default that Charlie had thus far been able to avoid.[141] Charlie may even lose existing credit cards entirely.[142] Likewise, Charlie could be charged higher insurance premiums or even lose insurance—life, property, or health—altogether.[143] Bad credit, even if not the responsibility of the consumer, can prevent a consumer from obtaining student loans, delaying or even eliminating the opportunity for a college degree.

All of these consequences, although terrible in the aggregate, appear to be merely monetary. However, misattributed information can threaten not just finances, but liberty itself. If Charley develops a criminal history, that history could imperil Charlie. In one dramatic example of undermatching identifying information, a bank opened up an account in the name of an identity theft victim, even though the thief used only the victim's temporary license, which had no photograph, and the signature on the account application did not match the signature on the license.[144] The thief then wrote several bad checks and the defrauded

---

account for an identity thief in the plaintiff's name and continued to report the account as hers even three years after it appeared to have acknowledged its error).

140 *See, e.g.*, Rhodes v. Ford Motor Credit Co., 951 F.2d 905, 905-06 (8th Cir. 1991) (granting creditor's motion for summary judgment on FCRA claim based on lender's false report that borrower had defaulted on her car loan payments, an error that caused her to be rejected for another car purchase).

141 *See* Patrick McGeehan, *Soaring Interest Compounds Credit Card Woes for Millions*, N.Y. TIMES, Nov. 21, 2004, at sec. 1, col. 5, p. 1.

142 *See* McMillan v. Experian, 170 F. Supp. 2d 278, 282 (D. Conn. 2001) (defendant had merged records of the plaintiff's son, who had the same name as the plaintiff, into the plaintiff's report, leading a credit card company to terminate plaintiff's card and an insurer to deny insurance).

143 For example, in *Boris v. ChoicePoint Servs., Inc.*, 249 F. Supp. 2d 851, 855 (W.D. Ky. 2003), a consumer reporting agency falsely ascribed to the plaintiff five different claims that she had not made, leading her insurance company to send her a nonrenewal notice. *See also* Felis v. Greenberg, 51 Misc. 2d 441, 443, 275 N.Y.S.2d 288, 290 (Sup. Ct. 1966) (upholding claim against physician where physician had reported false information to the Medical Information Bureau, a data aggregator, which led to the plaintiff's insurer cutting off the plaintiff's disability benefits).

144 Patrick v. Union St. Bank, 681 So. 2d 1364, 1365 (Ala. 1996).

merchants sought recovery, which led to warrants being issued in eleven different jurisdictions for the victim's arrest. Although the victim was able to get those warrants of which she learned dismissed by showing that the signatures on the checks did not match hers, she was eventually arrested on other warrants and imprisoned in four different jurisdictions over a period of ten days before finally winning her release.[145] Similarly, a check cashing service falsely imputed to a store clerk that a customer was part of a "fraud ring," which caused the customer to be arrested and imprisoned.[146] This case illustrates the difficulties of correcting such misinformation; the consumer stayed imprisoned for ninety days, even though the agency learned within one day that the information was incorrect.[147]

Nonetheless, monetary consequences are more common. However, those consequences may arise not as a direct result of the record's presence in the biography, but from the impact of that record on a person's credit score. The mismatched information may not even appear directly before a creditor. Users will make decisions based not on a reading of the entire report, but on the basis of an individual's credit score, an algorithm that numerically weighs the information about a consumer.[148] The Fair Isaac Corporation produces credit scoring software that creditors use to determine access to credit and pricing of credit for consumers.[149] That score can determine whether a consumer receives credit and, if so, at what price.[150] A score too low will render a

---

145 *Id.* A similarly sinister version of identity theft is criminal record identity theft, where an impostor commits one or more crimes in the victim's name by providing the victim's identity to law enforcement when caught. *See* Beth Givens, Identity Theft: The Growing Problem of Wrongful Criminal Records, Presentation at the SEARCH National Conference on Privacy, Technology and Criminal Justice Information in Washington, D.C. (June 1, 2000), http://www.privacyrights.org/ar/wcr.htm; *see also* Michael W. Perl, Comment, *It's Not Always About the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft*, 94 J. CRIM. L. & CRIMINOLOGY 169, 169-71 (2003) (discussing criminal record identity theft and "'reverse criminal record identity theft'" where the thief uses the victim's personal information to hide the thief's own criminal record).

146 Haque v. CompUSA, Inc., No. 02-10345-RWZ, 2003 WL 117986, at *2 (D. Mass. Jan. 13, 2003) (denying agency's motion to dismiss the consumer's FCRA claim; the court also ruled that the plaintiff stated a claim for false imprisonment against the agency).

147 *Id.* at *1.

148 *See supra* text accompanying notes 38-41.

149 *See* CREDIT SCORE ACCURACY, *supra* note 86, at 41 (noting the tremendous impact of credit scoring companies on the access to "essential consumer services," and pointing out that "[m]any decision makers who use scoring systems to evaluate consumer applications do not even understand the systems themselves . . . .") (emphasis omitted).

150 My Fico, http://www.myfico.com (last visited Jan. 13, 2007). The Fair Isaac Corporation Web site identifies interest rates available to consumers in various ranges of credit scores that fall between 500 and 850. *Id.*

consumer subject to the sub-prime loan market, at great increased cost to the consumer.[151] In fact, a score too low may even prevent a consumer from being able to open a checking account at a bank.[152] The practice of feeding information into an algorithm to produce a number—one three digit number—that purports to assess an individual's worthiness to participate in future transactions also has increased the power of false data on consumers' lives. Under the general rule of garbage-in-garbage-out, a false piece of information associated with a consumer may well drag down that consumer's credit score, depending on the weight the credit scoring algorithm assigns to that item. However, neither the user nor the individual will know from the score itself that a false item deflated it.

One study estimated that one in five consumers was likely to be assigned a lower score than deserved because of errors or inconsistencies in that consumer's credit history.[153] The study further estimated that inaccurate financial biographies put tens of millions of consumers at risk of suffering higher-priced credit, or even being eliminated from the credit market.[154] Many such consumers cannot afford the damage that the mismatched information will do to their ability to pay their bills. While a consumer could choose to pay cash for everything, even going "off-the-grid" will not avoid the consequences of the information, and a consumer may well be stuck with denying the acts of his or her distorted image projected from the computerized record. Furthermore, to the extent that an individual's life is held up by a false credit item, the individual is not fully participating in the benefits of being an American consumer. Thus, mismatching of transactions can have a devastating impact on a person's ability to find work and shelter and to live affordably. As discussed below, it can also cause intangible but nonetheless genuine damage to personality and dignity.

2. Damage to Personality and Dignity

Transactions with others express an individual personality, defined by Margaret Radin as "a continuing character structure encompassing future projects or plans, as well as past events and feelings."[155] Obviously, a transactional biography can reveal past events. However,

---

151 *See* CREDIT SCORE ACCURACY, *supra* note 86, at 37-38.

152 Harriet Johnson Brackey, *Banks Check Potential Customers' Credit*, MIAMI HERALD, Dec. 5, 2004, at 1E; *see also* HENDRICKS, *supra* note 39, at 3-4.

153 *See* CREDIT SCORE ACCURACY, *supra* note 86, at 37.

154 *See id.* at 36-37.

155 Margaret Jane Radin, *Property and Personhood*, 34 STAN. L. REV. 957, 968 (1982).

the individual items can also reveal a personal gestalt that can hold enough of the essence of an individual to predict future projects or plans—after all, that is why third parties seek it, to predict future behavior. Thus, the record of transactions radiates an image of personality, though perhaps an imperfect one. Outsiders can compute from the individual acts an estimate of that person's character with respect to a particular trait—in other words, a reputation. As individuals, we express our personalities through our transactions: the stores we patronize, the items we buy, from books to toothpaste, the charities and causes that we support, the persons we call, and even, or perhaps especially, the Web sites we visit. In the digital age, that self is constructed for many interested watchers by external automated processes. When the choices of another are attributed to us, we lose control over the images that others believe faithfully represent our choices.

While reputation is external to the self, existing in the minds of others,[156] under the Kantian characterization, dignity is a matter of intrinsic worth that recognizes that each person merits being acknowledged as an "individual and independent personality."[157] By recognizing dignity we acknowledge a person's right to freely develop that person's personality.[158] Arguably, information aggregation itself violates human dignity by depersonalizing individuals and treating them as mere objects to some other ends.[159] However, damage to dignity worsens when the information is misaggregated to attribute a deed to the wrong doer.

To mischaracterize someone's personality is to injure his dignity. Robert C. Post writes of the concept of reputation as dignity, drawing on the sociological research of Erving Goffman to argue that dignity "is a ritual and ceremonial aspect of the self that we associate with the self's integrity[.]"[160] The observer of an exchange between a person and a

---

156 Heyman, *supra* note 16, at 1325.

157 *See* IMMANUEL KANT, THE METAPHYSICS OF MORALS 255 (Mary Gregor trans. 1991); *see also* Edward J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, 1997 UTAH L. REV. 963, 972 n.36 (citing *Life Imprisonment Case*, 45 BVerfGE 187, 228 (1977), *translated in* DAVID P. CURRIE, THE CONSTITUTION OF THE FEDERAL REPUBLIC OF GERMANY 314 (1994)); William A. Parent, *Constitutional Values and Human Dignity*, *in* THE CONSTITUTION OF RIGHTS: HUMAN DIGNITY AND AMERICAN VALUES 47 (Michael J. Meyer & W.A. Parent eds., 1992).

158 Eberle, *supra* note 157, at 972.

159 *Id*. at 1001.

160 *See* Robert C. Post, *The Social Foundations of Defamation Law: Reputation and the Constitution*, 74 CAL. L. REV. 691, 708-10 (1986). Post also described the concept of

speaker who speaks falsely about that person may have to choose which image—the true or the false—to believe.[161] If the observer sides with the speaker, the person is discredited (literally, as far as creditworthiness is concerned).[162] The person becomes subject to "'exclusion from belonging as a respected and responsible' member of society[,]" losing dignity.[163] Even where the false attribution of an action does not cause substantive harm to a person's reputation, as Steven Heyman points out, it can "nevertheless violate her dignity as an autonomous being," regardless of whether the specific item of information is derogatory or not, by treating that person as a "mere object rather than an active subject."[164]

However, the attribution of events to a person who did not do them injures dignity in a manner different from that of depersonalization, of person as object. By falsely attributing an event to an actor, the attributor damages the individual's right to self-determination by inflicting the consequences of the false attribution on the individual. The individual may be denied the ability to have the same interactions with others that would otherwise be possible and the individual's realm of choices may be unjustly circumscribed. This is because others may choose to change their own course of action based on the false information, either choosing not to play with the misrepresented individual or by changing the terms on which they will play. The individual's ability to author his or her future is hampered by not his or her own past, but by that of someone else; personality as well as dignity is damaged. However, the primary legal structures that exist to protect one's reputation for purposes of participating in the marketplace do not sufficiently motivate data providers and aggregators to identify transactions more accurately, as discussed below.

III. THE FAIR CREDIT REPORTING ACT AND ITS FLAWS

However much misattributed information may damage reputations, thereby inflicting not only tangible financial damage, but also damage to personality and dignity, victims of misattributed information have little

---

reputation as property, earned through one's own hard work, which is treated as a private good and accorded value by the market. *Id.* at 693-99.

161 *Id.* at 711.

162 *Id.*

163 *Id.* (quoting Kenneth Karst, *Paths to Belonging: The Constitution and Cultural Identity*, 64 N.C. L. REV. 303, 323 (1986)).

164 Heyman *supra* note 16, at 1339. Of course, if a false statement about someone does not cause injury to that person's reputation, it is not defamatory. *Id.* Nonetheless, the statement may be actionable under the tort of false light invasion of privacy, which Heyman describes as "protecting the dignitary dimension of reputation." *Id.*

effective recourse for these injuries, despite the legal maxim *ubi jus, ibi remedium*, for every right there shall be a remedy.[165] Protection of reputation was originally the province of common law, through the torts of defamation and false light.[166] However, now the federal FCRA (or "the Act") is the primary legal tool designed to promote the accuracy and integrity of transactional biographies, at least with respect to personal information used for credit, insurance, or employment purposes.

But this Act inadequately protects individuals from the consequential and emotional damages caused by misattributed acts for several reasons. First, it only imposes meaningful accuracy requirements on data providers and data aggregators *after* the false information has already been reported.[167] Second, the Act overprotects data aggregators and providers by limiting private suits, preempting state laws, and giving qualified immunity from state torts to those who must comply with the Act.[168] Though that qualified immunity mimics a privilege recognized widely at common law in defamation actions, courts have read the Act's version with far too much deference to the industry's interests, insufficiently valuing the impact bad information has on a modern consumer's life.

The FCRA was developed to solve the problem of misattributed information. More than thirty-five years ago, once computers began to take over the chores of aggregating and sorting data, Congress began to recognize the power of widely available, aggregated data, the lack of power individuals had over the collection and use of such data, and the likelihood that some data could get assigned to the wrong person. [169]

---

165 BLACK'S LAW DICTIONARY 1761 (8th ed. 1990).

166 *See* W.S. Holdsworth, *Defamation in the 16th and 17th Centuries*, 40 L.Q. REV. 302, 303-05 (1924) (discussing the development of defamation in the common law courts of England).

167 *See infra* text accompanying notes 176-93.

168 *See infra* text accompanying notes 235-39.

169 One member of Congress expressed the fears of many:

> Undoubtedly the computerization of personal information about millions of individuals gives this subject greater importance and urgency then it had in the days when the average businessman knew his customers personally and knew the good credit risks from the bad, and the insurance agent was an old acquaintance who knew the probably good actuarial risks from the probably bad ones. Today, such data is almost completely second hand, third hand or even more distant and impersonal, and it is almost impossible to find a human being to unravel a computer error once it's made. When the computer is half a continent away and connected to the store by electronics, the

Senator Proxmire, who led Congress in this reform effort, argued that "We certainly would not tolerate a Government agency depriving a citizen of his livelihood or freedom on the basis of unsubstantiated gossip without an opportunity to present his case. And yet this is entirely possible on the part of a credit reporting agency."[170] Eventually Congress passed the original FCRA.[171] However, the accuracy provisions of the Act and many courts' interpretations of those provisions have not solved the problem of such "gossip" and have not kept up with modern information practices.

Currently, the FCRA[172] regulates the reporting of a broad category of records: those that bear on an individual's credit, character, general reputation, or personal characteristics,[173] if an agency communicates the report for the purpose of determining a consumer's eligibility for credit, insurance, or employment.[174] Anyone with a business need for the information may obtain it.[175] Given that so many transactions and so much detail about those transactions are being stored and analyzed, the volume of information subject to the Act expands every day.[176]

A. The Fair Credit Reporting Act's Accuracy Provisions

The Act's most significant flaw is that it imposes meaningful accuracy requirements only *after* a false and negative item has been reported, has already been put into the data sea. However, given that

---

> remoteness of the customer from the real arbiter of his credit worthiness becomes even more pronounced.

Hearings Before the Subcommittee on Consumer Affairs of the Committee on Banking and Currency on H.R. 16340, 91st Cong., 2d Sess. 1 (1970) (remarks of Congresswoman Leonor Sullivan).

170 115 CONG. REC. S2412 (1969) (remarks of Senator Proxmire). The discussions around the Act also revealed some techno-phobia:

> with the trend toward . . . the establishment of all sorts of computerized data banks, the individual is in great danger of having his life and character reduced to impersonal "blips" and key-punch holes in a stolid and unthinking machine which can literally ruin his reputation without cause, and make him unemployable.

116 CONG. REC. S36570 (1970) (remarks of Representative Sullivan). Inaccurate and misleading information was seen as the most serious problem in the credit reporting industry, and the impact of even a small percentage of errors was recognized: "Everyone is a potential victim of an inaccurate credit report. If not today, then perhaps tomorrow." 115 CONG. REC. S2411 (1969). As Senator Proxmire noted, even a one percent error rate would lead to a million citizens having "reputations . . . unjustly maligned." *Id.*

171 Pub. L. No. 91-508 (1970).

172 FCRA, 15 U.S.C. §§ 1681-1681x (2000), *amended by* Pub. L. No. 108-159 (Dec. 4, 2003).

173 15 U.S.C. § 1681a(d).

174 *Id.* §§ 1681(a)(d)(1)(A)-(B).

175 *Id.* § 1681b(a)(3)(F).

176 *See supra* text accompanying notes 30-33.

digitized data is far more available, accessible, duplicatable, and transmittable than old paper records, once a false record has been put into the data sea, it is very hard to ever completely cull it out.

To provide an overview of the process regulated by the Act, as discussed above, a record of the sort covered by the Act generally originates with a business or governmental entity, which usually is the creator of an electronic record of a transaction, or at least maintains the record in that form.[177] The business provides the information, along with identity markers for the responsible individual, to a data aggregator, called a consumer reporting agency in the Act.[178] For example, a bank may report that a car loan belongs to the identified consumer and that the consumer has defaulted on it. The aggregator, or agency, collects the information and warehouses it in vast databanks, ready to provide it to any customer who asks for it.

The Act is designed to impose meaningful accuracy standards only after inaccurate information has already been provided by a data provider and reported by a data aggregator. The Act permits the original data provider, called a furnisher under the Act, to furnish nearly any item in a consumer's name without first verifying that it belongs to that consumer.[179] But the Act only prohibits the furnisher from furnishing information that the furnisher either "knows or has reasonable cause to believe" to be inaccurate.[180] A furnisher only has "'reasonable cause to believe that an item of information is inaccurate'" if the furnisher has "specific knowledge, *other than solely allegations by the consumer*, that would cause a reasonable person to have substantial doubts about the accuracy of the information."[181]

Although Congress supplemented the initial accuracy standard in 2003 to prohibit a provider from furnishing information that a consumer has notified the provider to be inaccurate,[182] the supplement is largely

---

177 *See supra* text accompanying notes 19-23.

178 15 U.S.C. § 1681a(f). The FCRA defines a consumer reporting agency to be "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . . ." *Id.*

179 15 U.S.C. § 1681s-2, *amended by* Pub. L. No. 108-159, 117 Stat. 1952 (2003).

180 *Id.* §§ 1681s-2(a)(1)(A), 1681s-2(a)(1)(D), *amended by* Pub. L. No. 108-159, § 312(b), 117 Stat. 1952 (2003).

181 *Id.* § 1681s-2(a)(1)(D), *added by* Pub. L. No. 108-159, § 312(b), 117 Stat. 1952 (2003) (emphasis added).

182 *Id.* § 1681 s-2(a)(1)(B), *amended by* Pub. L. No. 108-159, § 312(e), 117 Stat. 1952 (2003).

cosmetic because of the qualifications that undermine it.[183] In any event, none of the standards imposed on data providers at the point of initially furnishing data are meaningful because Congress specifically prohibited injured consumers from the ability to enforce them.[184]

Thus, the agency acquires information that likely has not been subjected to any scrutiny, let alone verified. The agency acquires the information, either electronically or via magnetic tape from the provider, and stores it electronically, where it sits until needed for a report. Just as the Act imposes a relatively weak accuracy requirement on data providers at the point of initial provision, the Act places only loose limits on aggregators that then report the information. When a subscriber requests a report on a particular consumer, the aggregator, the consumer reporting agency, must only follow "reasonable procedures to assure maximum possible accuracy" of the information that it returns to the subscriber.[185] The provision does not in fact require agencies to ensure the maximum possible accuracy of every item of information, or to do much if anything to match, verify, or cross-check the information.[186] Some courts have ruled that an agency need only look beneath the surface identification if it has reason to suspect the accuracy of a source of information.[187] Furthermore, many courts have curtailed the effect of

---

[183] *Id.* § 1681s-2(a)(6)(B)(i). The furnisher need only comply with this second accuracy obligation if the consumer notifies the furnisher at the furnisher's designated address for such information. *Id.* The Act exempts furnishers from the obligation to avoid furnishing inaccurate information if the furnisher has specified to a consumer an address that the consumer can use to notify the furnisher that the information is inaccurate. *Id*. § 1681s-2(a)(1)(C). However, the Act does not require furnishers to provide such an inaccuracy-notice address. *Id.* A furnisher that learns that it has furnished inaccurate data about a consumer must also notify the agencies to which it has furnished the information of that knowledge and correct the inaccuracy. *Id.* § 1681s-2(a)(2). This requirement applies only to furnishers who furnish consumer information "regularly and in the ordinary course of business." *Id*. § 1681s-2(a)(2)(A).

[184] *Id*. § 1681s-2(d), *amended by* Pub. L. No. 108-159 § 312(e), 117 Stat. 1952 (2003).

[185] *Id*. § 1681e(b).

[186] FTC Official Staff Commentary § 607 item 3A, http://www.lawdog.com/CREDIT/crta410.htm (last visited Jan. 13, 2007); *see also* Smith v. Auto Mashers, Inc., 85 F. Supp. 2d 638, 641 (W.D. Va. 2000). An agency does not violate this provision "simply by reporting an item of information that turns out to be inaccurate[,]" and dismissing the claim of the plaintiff, who was fired after an agency reported that he'd failed a drug screen, when in fact he had not. *Smith*, 85 F. Supp. 2d at 641.

[187] *See, e.g.*, Dalton v. Capital Associated Indus., 257 F.3d 409, 416 (4th Cir. 2001); Pinner v. Schmidt, 805 F.2d 1258, 1262 (5th Cir. 1986), *cert. denied*, 483 US. 1022 (1987) (where agency knew of personal dispute between consumer and person reporting the contested data to the agency, agency should not have relied on that person's verification of the data once the consumer disputed it); Bryant v. TRW, Inc., 689 F.2d 72, 77-78 (6th Cir. 1982); Thomas v. Gulf Coast Credit Servs., Inc., 214 F. Supp. 2d 1228, 1234-35 (M.D. Ala. 2002) ("blind reliance" on secondary sources that each offered the same inaccurate information

the accuracy requirement by incorporating a balancing test clearly not in the text of the Act, weighing "the potential that the information will create a misleading impression against the availability of more accurate [or complete] information and the burden of providing such information."[188] Between the provision itself and the interpretations of it, the Act signals to aggregators and furnishers that they can employ a default rule of merely passing through, unvetted, details about a transaction in a consumer's name without fear of liability.

It is only *after* an individual has learned that an agency has falsely charged him or her with negative data that the individual can require an aggregator to examine the data. The maligned individual may demand that the agency "reinvestigate" the inaccurate information, a term in the Act that inaccurately suggests that the agency investigated the item to begin with.[189] The agency then can choose between reinvestigating the information and deleting it.[190] In fulfilling this accuracy obligation, the agency must make a good faith effort to determine the accuracy of the disputed item[191]—that is, the agency must do more than merely reconfirm, *pro forma*, the identity of the consumer with the business that originally provided the data.[192] Thus, in theory, where another's deeds are wrongly attributed to an individual, the agency must make a good

---

about identity theft victim was not reasonable); Swoager v. Credit Bureau, 608 F. Supp. 972, 974 (M.D. Fla. 1976) (merely parroting furnisher's information did not meet agency's obligation of reasonable reinvestigation).

188 Koropoulous v. Credit Bureau, Inc., 734 F.2d 37, 42 (7th Cir. 1984) (vacating summary judgment in favor of agency); Zotta v. NationsCredit Fin. Servs., 297 F. Supp. 2d 1196, 1203 (E.D. Mo. 2003) (agency must do more than simply correctly report the information given to it by the provider); *see also* Bryant v. TRW, Inc., 487 F. Supp. 1234, 1237 (E.D. Mich. 1980) (holding that this provision may require an agency to keep track of the accuracy of its sources in order to prevent vaguely identified records from poisoning an individual's file).

189 15 U.S.C. § 1681e. Presumably the term "reinvestigation" is used because the agency should have previously done some investigation in accepting the data to begin with, as required by § 1681e.

190 *Id*. § 1681(a), *amended by* Pub. L. No. 108-159, 117 Stat. 1952 (2003).

191 F.T.C. Official Staff Commentary § 611 item 2, http://www.lawdog.com/CREDIT/crta414.htm (last visited Jan. 13, 2007).

192 Cushman v. Trans Union Corp., 115 F.3d 220, 225-26 (3d Cir. 1997) (stating that agency may not merely rely on a creditor's information when an identity theft victim challenged an account as not being his, and reversing lower court's judgment for agency); Zala v. Trans Union, L.L.C., No. 3:99-CV-0399, 2001 WL 210693, at *5 (N.D. Tex. Jan. 17, 2001) (agency must inquire both of original creditor and of available public records). A recent addition to the Act specifies that the agency's reinvestigation must be "reasonable." 15 U.S.C. § 1681i(a)(1)(A) (Supp. III 2003), *amended by* Pub. L. No. 108-159 § 317, 117 Stat. 1952 (2003).

faith effort to verify the attribution with the provider once the injured individual notifies the agency of the mismatch.[193]

The language of the reinvestigation provision creates a vision of a thoughtful and professional clerk evaluating the consumer's file in earnest consultation with the original data provider. However, notwithstanding the responsibility, in fact the reinvestigation process is nearly as automated as the transmission of the original information to the agency. The agency will usually send the provider a Consumer Dispute Verification form, whose automated form is known as an Automated Consumer Dispute Verification Form.[194] This process reduces a defamed consumer's anguished and detailed description of an error to a generalized code.[195]

Once a data provider, a furnisher, receives this form, it must conduct a reasonable investigation of the inaccurate information.[196] If the original

---

193 *Cushman*, 115 F.3d at 225; Henson v. CSC Credit Servs., 29 F.3d 280, 286-87 (7th Cir. 1994).

194 *The Role of the FCRA in the Credit Granting Process Before the Subcomm. on Financial Institutions and Consumer Credit*, 108th Cong. 6 (2003) (statement of Harry Gambill, Chief Executive Officer, Trans Union, L.L.C.). According to one representative of a national consumer reporting agency, 52% of its data providers use the automated consumer dispute verification system. *Id.*; *see also* Anderson v. Trans Union, L.L.C., 345 F. Supp. 2d 963, 966-67 (W.D. Wis. 2004) (describing automated process); McKeown v. Sears Roebuck & Co., 335 F. Supp. 2d 917, 926 (W.D. Wis. 2004) (same); Graham v. CSC Credit Servs., Inc., 306 F. Supp. 2d 873, 876-77 (D. Minn. 2004) (same).

195 HENDRICKS, *supra* note 39, at 98-99 (describing the verification process). For example, in a case where an agency misattributed a report of death to the plaintiff, the agency sent an automated consumer dispute verification form with a two character code that produced an automatic written message, "'special comment, compliance condition and/or remarks message disputed. Consumer not liable for acct. (i.e., ex-spouse, business). If liable provide complete ID and ECOA [Equal Credit Opportunity Act] code.'" *McKeown*, 335 F. Supp. 2d at 926.

196 15 U.S.C. § 1681s-2(b) (2000), *amended by* Pub. L. No. 108-159, 117 Stat. 1952 (2003). The provider must reasonably investigate whether the provider can verify the item. Johnson v. MBNA Am. Bank, NA, 357 F.3d 426, 430 (4th Cir. 2004) (rejecting provider's argument that the Act requires only a "minimal duty" to "briefly review" its records); *see also* Wade v. Equifax, No. 02-C-3205, 2003 WL 22089694, at *4 (N.D. Ill. Sept. 8, 2003) (rejecting claim against provider who had reported an account opened by an identity thief as being the plaintiff's, even though the plaintiff's name, Lori Wade, differed substantially from the name the thief used, Lori White); Olwell v. Med. Info. Bureau, No. 01-1481 JRTFLN, 2003 WL 79035, at *5 (D. Minn. Jan. 7, 2003) (denying provider's motion for summary judgment where insurance company reported plaintiff as having failed a test that detected smoking on the grounds that the provider could be required to contact outside services to comply with its obligation to reinvestigate the information); Malm v. Household Bank (SB), N.A., No. 03-434OADMAJB, 2004 WL 1559370, at * 5 (D. Minn. July 7, 2004) (dismissing claim where provider did not learn that consumer's wife had forged his signature on credit card); Agosta v. Inovision, Inc., No. 02-806, 2003 WL 22999213, at *5

provider cannot verify the item, the provider must "take steps to" modify, delete, or block the information.[197] In theory, any mistranscription or misattribution error should be caught here, because an inaccurately attributed record would not be verifiable. In any event, the provider must then notify the agency of the results of its investigation.[198] Then the agency must not only notify the individual of the results of the search, but also the provider when the agency corrects or deletes inaccurate information as a result of the reinvestigation.[199]

In 2003, as part of an overhaul of the Act, Congress took steps to curtail mismatching of information.[200] However, instead of addressing the careless matching practices of providers and agencies that lead to so much poisoning of financial biographies, it focused on the subset of such information arising from identity theft. Consumers may now require an agency to put a fraud alert in any report on the consumer. The alerts also impose new responsibilities on users to verify the identity of anyone who applies for credit in the name of the victim.[201] Furthermore, nationwide credit reporting agencies will have to block theft-related

---

(E.D. Pa. Dec. 16, 2003); Betts v. Equifax Credit Info. Servs., Inc., 245 F. Supp. 2d 1130, 1135 (W.D. Wash. 2003) (denying provider's motion for summary judgment where furnisher, who sought to collect a debt incurred from towing an abandoned car, reported the debt as belonging to the plaintiff, although plaintiff had successfully claimed in different suit that she did not own the car); Kronstedt v. Equifax CSC, No. 01-C-0052-C, 2001 WL 34124783, at *7, *17 (W.D. Wis. Dec. 14. 2001) (denying provider's motion for summary judgment where provider confirmed debt even though it had been notified that the plaintiff was a victim of identity theft); Bruce v. First U.S.A. Bank, 103 F. Supp. 2d 1135, 1143-44 (E.D. Mo. 2000) (denying provider's motion for summary judgment where provider had reported a card taken out by the plaintiff's ex-wife as belonging to plaintiff, even though he had repeatedly notified the issuer of the fraud and the provider's own investigation showed that the signatures on the account application did not match plaintiff's).

197 15 U.S.C. § 1681s-2(b)(1)(E). The provider need only do this for the purpose of reporting information to the agency. *Id.*

198 *Id.* § 1681s-2(b)(1)(C).

199 *Id.* § 1681i(a)(5)(A), *amended by* Pub. L. No. 108-159, § 314(a), 117 Stat. 1995 (2003).

200 *Id.* § 1681c-1 (Supp. III 2003); *see also* 16 C.F.R § 603.2 (2006) (defining the terms "identity theft" and "identifying information").

201 15 U.S.C. § 1681c-1(h)(1)(B) (Supp. III 2003), *added by* Pub. L. No. 108-159, § 112, 117 Stat. 1955 (2003). The Act as amended also requires businesses that have done business with an identity thief in the victim's name to provide the victim with information about the transaction, such as providing the victim with the thief's credit application. *Id.*, *added by* Pub. L. No. 108-159, § 151, 117 Stat. 1961 (2003). However, the business does not become obligated to cooperate until the victim has proven his or her own identity to the business's satisfaction. *See id.* § 1681g(e)(2). The irony being, of course, that if the business had demanded appropriate identification of the thief's identity, the victim would likely not have become a victim. *Id.*

debts from their files.[202] Once a consumer submits an identity theft report to a provider of bad data, the provider must cease furnishing the fraudulent information in the victim's name unless the provider subsequently "knows" that the information is correct.[203] These provisions have the same flaw as the general accuracy provisions that apply to ordinary data: they focus on the time after a data provider and data aggregator have already attributed the thief's information to the victim, after the digitized records have been reported.

In short, the tepid standards that govern the initial provision of information to aggregators and to those aggregators' subscribers give data providers and aggregators a free bite of the apple. They can sort of shoot haphazardly for accuracy without having to take steps to target it. Thus, the Act in practice has not effectively filtered bad information from the pool of consumer data, nor has it protected consumers from the harmful effects of such data.[204] The most meaningful accuracy check—the reinvestigation required of agencies and providers—does not arise until after a consumer challenges a piece of misattributed information. Realistically a consumer is not going to learn that an aggregator has distorted the consumer's biography with a mismatched record until the aggregator has reported the item to a third party, a third party who is likely checking the individual's biography to determine the individual's worthiness for a particular benefit. Thus, a consumer has to suffer the reporting of false information before being entitled to any review of the substance of the information. By that time, the consumer may well have suffered consequences to finances and to personal dignity that cannot necessarily be undone. In the fictional example described above, Charlie would suffer the loss of a mortgage and possibly even a job itself. He could be denied insurance, and may even be arrested, all before being

---

[202] *Id.* § 1681c-2(a) (Supp. III 2003), *added by* Pub. L. No. 108-159, § 152(a), 117 Stat. 1964 (2003). The agency must notify the provider of the blocked information that it may have arisen from an identity theft. *Id.* § 1681c-2(b)(1). Once notified, the data provider must implement procedures to prevent them from re-providing the information. *Id.* § 1681s-2(a)(6), *added by* Pub. L. No. 108-159, § 154, 117 Stat. 1966 (2003). Although the Act allows the agency to unblock the information under certain circumstances, the agency must notify the consumer that it is doing so. *Id.* § 1681c-2(c)(2), *added by* Pub. L. No. 108-159, § 152, 117 Stat. 1964 (2003).

[203] *Id.* § 1681s-2(a)(6)(B) (Supp. III 2003), *added by* Pub. L. No. 108-159, § 154, 117 Stat. 1952 (2003). The Act as revised by the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003), also requires a furnisher to put in place reasonable procedures to respond to any notice that it receives from a consumer reporting agency that a consumer has blocked identified information from the consumer's report as resulting from identity theft. *Id.* § 1681s-2(a)(6)(A), *added by* Pub. L. No. 108-159, § 154 (2003).

[204] *See supra* text accompanying notes 61-63.

able to compel the data aggregator and the data provider to correct the mismatch, to get them to disconnect him from the discrediting act.

A misattribution may prevent the consumer from being able to fully participate in the marketplace at a critical time in that consumer's life.[205] By the time the consumer learns of the error, not only has his reputation been wrecked by the false information, the attribution of that information to him has hampered his ability to live his life forward based on his past. By delaying its meaningful accuracy test, the Act allows agencies and furnishers a free pass that can be painfully costly to the defamed consumer.

Such weak protections from mismatched information might have been appropriate in 1970 when the FCRA was first enacted.[206] At that time, many records would have been on paper and reported on tape. Though computerization did motivate Congress to enact the legislation, data technology was still in its infancy and the Internet was largely just a gleam in the eyes of a few dreamers.[207] A free bite of the apple of inaccuracy may have been justified then, as so many errors could only have been caught through the painstaking process of human visual inspection.

Courts, however, continue to interpret the Act as if the records were arduously searched by hand, rather than easily by machine, and construe the already mild obligation of agencies to use "'reasonable procedures to assure maximum possible accuracy'" before initially reporting a negative item in a consumer's name in ways that wholly fail to promote identification accuracy.[208] *Crabill v. Trans Union, L.L.C.,* [209] and *Sarver v. Experian Information Solutions*,[210] both from the Seventh Circuit, exemplify the stale application of analog standards of recklessness. In *Crabill*, the defendant, a national consumer reporting agency, repeatedly misattributed to the plaintiff information about transactions belonging to

---

[205] *See* CREDIT SCORE ACCURACY, *supra* note 86. One study found, for example, that such exclusions from commerce are particularly likely to happen during period of heavy volume, such as when interest rates provoke a rash of refinancings. *Id.*

[206] Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104-208 § 2413(a)(2), 110 Stat. 3009 (1996). Standards for furnishers were not imposed until 1996. *Id.*

[207] *See* The Internet: A Short History of Getting Connected, www.fcc.gov/omd/history/intenet/ (last visited Jan. 13, 2007).

[208] Sarver v. Experian Info. Solutions, 390 F.3d 969, 971 (7th Cir. 2004); Crabill v. Trans Union, L.L.C., 259 F.3d 662, 663 (7th Cir. 2001).

[209] 259 F.3d at 663.

[210] 390 F.3d at 972.

the plaintiff's brother.[211] The agency did so even though the brothers had different first names (John versus Jerry) and different social security numbers.[212] Their dates of birth, a piece of data that individuals do not often mistake, were thirteen months apart.[213] Given this knowledge, the agency's attribution of both sets of records to the plaintiff not only overlooked the possibility of harm, but rashly ignored it. In the parlance of this Article, the agency used fuzzy matching.[214]

Nonetheless, Judge Posner, writing for the unanimous panel, excused the misattribution, noting that not only did the first names begin with the same letter, but that the brothers' social security numbers differed by just one number.[215] The court agreed with the agency that someone could have mistranscribed the names and number, which could lead to the possibility that the transactions involved could in fact have been incurred by either brother.[216] This possibility, according to the court, justified the mismatching.[217] Although the court acknowledged that Trans Union could have programmed its computer differently to match less loosely, it condoned the oversized net Trans Union used to pull the plaintiff's information from its databases, finding that the agency could reasonably report the transactions of both brothers as those of each one individually.[218]

The *Crabill* decision permits data aggregators a level of imprecision that conflicts with day-to-day experience in the modern digital world, as opposed to the old analog one. Most of us are accustomed to making exacting matches between strings of characters. We expect that if we miss one digit of a PIN, transpose two characters of a password, or skip one numeral in an account number, access will be denied. Instead of requiring that level of exactitude that is routine in our digital, character-string-driven world, the *Crabill* court essentially allowed the defendant to play by 1970 capability rules. As a result, each brother was denied the right to be judged by his own biography and, instead, must submit to being judged based on deeds done by another. The plaintiff lost control over the image of his personality presented to others.

---

211 259 F.3d at 663.

212 *Id.*

213 Supplemental Brief of Appellee at *2, Crabill v. Trans Union Corp., No. 00-2078, 2001 WL 34105114 (7th Cir. June 18, 2001).

214 *See supra* text accompanying notes 139-43.

215 *Crabill*, 259 F.3d at 663.

216 *Id.*

217 *Id.*

218 *Id.* The court affirmed summary judgment for the agency on the plaintiff's FCRA claim. *Id*. at 667.

The *Crabill* court was persuaded by the aggregator's justification for fuzzy matching, that it increases accuracy by scooping up records actually attributable to the targeted individual, but that fail to precisely match the individual's identity markers because someone—the original recorder or the individual—mistranscribed one or more markers. However, aggregators that employ fuzzy matching for that reason could come even closer to their goal of a full and accurate portrayal of the person by cross-checking that pool of records against known matches, a task that would have been a great burden in the early days of the Act, but which would likely take nothing but a tweak of the existing algorithms and nanoseconds of computer time now. By overlooking all the benefits of modern data technology that allowed the agency to traffic in the mismatched records, the court failed to accord the benefits of that technology to the misportrayed consumer.

Cross-checking can also prevent misattribution by undermatching, where a record with identifying information insufficient to pinpoint it to a specific individual is tagged to the wrong person. An aggregator can compare the record with other information more closely matched to the individual, which can reveal an inconsistency that the aggregator should resolve before reporting any, especially negative, information. For example, a record of an account opened in 1965 should not be matched to an individual not born until four years later, regardless of the similarity between the names.[219] But internal inconsistencies can be more subtle. For instance, if an aggregator has a bankruptcy filing record with one person's name, the aggregator could check additional matching data before attributing it to the identity of a person who has the same name, but whose other records show minimal debt.[220] A report that differs substantially from one issued the previous month,[221] or is derogatory when previously the subject had an "excellent business and social reputation,"[222] should raise the need for additional verification.[223] One should be accountable for what one already knows and not hurt someone's reputation by disregarding that knowledge.

---

[219] Sheffer v. Experian Info. Solutions, Inc., No. 02-7407, 2003 WL 21710573, at *1 (E.D. Pa. July 24, 2003).

[220] Stewart v. Credit Bureau, Inc., 734 F.2d 47, 52 (D.C. Cir. 1984). The court ruled that reporting such a record notwithstanding this sort of inconsistency could be unreasonable. *Id.* at 51-52 (interpreting the FCRA).

[221] Bryant v. TRW, Inc., 689 F.2d 72, 77-78 (6th Cir. 1982).

[222] Roemer v. Retail Credit Co., 119 Cal. Rptr. 82, 88 (Ct. App. 1975) (upholding jury's finding that agency acted with malice).

[223] *Id.*

Notwithstanding the advances in data technology, courts have generally held that agencies need not review a report for such inconsistencies before issuing it. For example, in *Sarver v. Experian Information Solutions*, another Seventh Circuit opinion, the court rejected the claim of an individual to whom the agency had wrongly attributed the bankruptcy of another.[224] The court approved of an agency's mismatch of accounts that referred to a bankruptcy filing to the plaintiff, even though only those accounts, and no others associated with that plaintiff, were listed as having been "involved in bankruptcy."[225] Furthermore, the agency had not received any information of a bankruptcy judgment in the plaintiff's name.[226]

The plaintiff argued that given that only one set of accounts was involved in bankruptcy, in contrast to the many healthy accounts attributed to the plaintiff, the inconsistency should have alerted the agency to its attribution error, but the court disagreed.[227] In justifying the agency's failure to resolve the anomalies within the records attributed to the plaintiff, the court emphasized the 200 million names and addresses, the 2.6 billion trade lines, and the complexity of the system.[228] This reasoning overlooks that the very complexity of the system reveals the ability of the agency to control the high volume of individuals and records, and that ability should alert the agency to the high risk of misattributing information. The court ruled that the agency's failure to investigate the inconsistency was not unreasonable because the agency had no notice that the specific lender who had provided information about the impaired accounts was unreliable.[229] However, the question, in order to protect individuals from reckless attribution, should not be whether any single provider is unreliable. The question should have been whether *reporting* it as the plaintiff's without checking it, given the obvious inconsistency, was reckless. Where the agency was aware of the risk of misattribution from fuzzy matching, and that matching produced a record that was unlike the others, a jury should decide whether the failure to take any steps to verify the anomalous data breached the FCRA's accuracy standard.

The *Sarver* court also reasoned that to require an agency to further investigate the accuracy of a consumer's records when an anomaly

---

224 390 F.3d 969, 972 (7th Cir. 2004).
225 *Id.*
226 *Id.*
227 *Id.*
228 *Id.*
229 *Id.*

appeared would impose "enormous" increased costs.[230] However, the court did not refer to any estimate of the costs or explain why an already complex system capable of making many comparisons among different records could not inexpensively adjust to cross-checking data when reliability was at issue. Furthermore, when an anomaly appears that would work to the consumer's detriment, an agency could simply decline to attribute the negative data should it not want to take the extra effort of verifying it. The decision allows the agency all of the benefits of its database technology with none of the responsibilities.

Similar to the court's disregard of the sort of precise matching expected in most non-face-to-face transactions today, this reasoning is out of date. The *Crabill* court should have understood that if the agency is able to "process[ ] over 50 million updates to trade information each day,"[231] it has the capability to analyze data and to do so quickly. The high-volume excuse may have been appropriate in an analog world, where the agencies relied on physical pieces of information that required a human being, rather than a computer, to read and understand them. Human beings read slowly, compared with computers, and make mistakes. However, the justification is no longer appropriate where a computer can quickly compare individual records for consistency. The *Sarver* court's construction ignores that the very technological tools that allow an agency to assemble a list of events for any one consumer can be tightened to cross-check for just such a discrepancy. The speed, storage capacities, and analytical capabilities of modern data processing systems rob a great deal of the wonder from the process. As mentioned above, Experian advertises that it maintains more than 65 terabytes—65 trillion bytes—of data on North American consumers and business.[232] The very fact that the agency is capable of those kinds of numbers shows the power it has over its data, as do the products the agencies market.[233] If the agency can harness that power for the benefit of data users, it should be able to direct it to the benefit of those individuals whose events give rise to the agency's income.

Not only do these decisions fail to recognize the aggregators' capacity to control data, they fail to reflect an understanding of the power of a bad biography in a modern, data-driven world. The stamina, accessibility, and duplicatability of all data and, for purposes of this

---

230 *Id.*

231 *Id.*

232 Corporate Fact Sheet, http://www.experian.com/corporate/factsheet.html (last visited Jan. 13, 2007).

233 *See supra* text accompanying notes 47-58.

discussion, bad data, give it much more power over the persons to whom it pertains than when such data was more functionally obscure.[234] To return to our fictional individual, once the calumny to Charlie Consumer is digitized, it is almost irreversible. Other aggregators will pick it up, store it, and report it. Users who would once not have sought such detailed information now will request reports and store the false information in Charlie's name. When challenged, the provider and aggregator may insist on attributing Charley's misdeeds to Charlie, and courts may hold that they can do so without violating the federal act intended to cleanse this sort of gossip out of the information sea. The original consumer's reputation, built as it is from a false image, will suffer among a much wider audience.

This power to cripple consumers' abilities to participate in standard life activities justifies a much higher standard of accuracy, not a lower one. This higher standard should arise at the initial reporting of negative information. Given the potential that a mismatched record has to disrupt someone's life, data providers and aggregators should ensure that a "digital dossier" contains only those events in which that individual actually participated.

B. The Fair Credit Reporting Act's Protection of Mismatchers

The FCRA is an unsatisfactory means for consumers to protect themselves from defamation not just because it imposes weak standards that several court decisions have further enfeebled. Even where a data provider or aggregator fails to meet the Act's standards, the Act protects them from the consequences in three ways: by prohibiting private suits for many infractions, by immunizing those in the consumer data industry from most state claims, and by preempting state laws that would require greater accuracy and accountability.[235] However, allowing those in the consumer data industry to traffic in information without fearing liability diminishes accuracy and may discourage data providers and aggregators from finding and using the sort of technology that would scrub misidentified events from the databases. Although some of these protections may have been justified in the nascent world of computerized records when Congress first enacted the Act, the last two major revisions to the Act have extended protections to private-sector aggregators even though technology justifies increasing liability instead.

---

234 *See supra* text accompanying notes 131-36.

235 15 U.S.C. § 1681h(e) (providing qualified immunity); *id*. § 1681s-2(c) (eliminating private causes of action for designated violations); *id*. § 1681t(b) (preempting designated state laws).

1. Limits on Private Suits

The aggregators garner, aggregate, and regurgitate information provided to them by their providers, the businesses that record their transactions with individuals. Thus, these providers' errors in furnishing data on a consumer will lead directly to inaccurate information disseminated by the agency. However, the rights that these FCRA provisions give with one hand they take away with another. The Act specifically provides that its civil claim sections[236] may not be used to enforce the obligation of providers to withhold information that they "know[ ] or ha[ve] reasonable cause to believe" is inaccurate, regardless of how egregiously a provider violates the provision.[237] Only designated federal agencies and state officials may enforce these rights.[238] Accordingly, without the sort of determined agency action that has not yet been forthcoming, the Act will do little to motivate data providers from taking care to match records of events with their doers.

Now, the Act allows consumers to enforce one accuracy provision against those data providers who attribute an event to the wrong consumer.[239] This provision, arising only after the provider has already

---

[236] *Id.* §§ 1681n-o (titled civil liability for willful noncompliance and civil liability for negligent noncompliance, respectively). The FCRA allows punitive damages if an actor "willfully" violates its responsibilities under the Act. *Id.* § 1681n(a). To show willful noncompliance, a plaintiff must show that a defendant "knowingly and intentionally committed an act in conscious disregard for the rights of others, but need not show malice or evil motive." Bakker v. McKinnon, 152 F.3d 1007, 1013 (8th Cir. 1998) (internal quotations omitted); *see also* Sapia v. Regency Motors, 276 F.3d 747, 753 (5th Cir. 2002); Northrop v. Hoffman of Simsbury, Inc., 12 Fed. Appx. 44, 50 (2d Cir. June 14, 2001); Cushman v. Trans Union Corp., 115 F.3d 220, 226 (3d Cir. 1997); Philbin v. Trans Union Corp., 101 F.3d 957, 970 (3d Cir. 1996); Pinner v. Schmidt, 805 F.2d 1258, 1263 (5th Cir. 1986), *cert. denied,* 483 U.S. 1022 (1987); Yohay v. City of Alexandria Employees Credit Union, Inc., 827 F.2d 967, 972 (4th Cir. 1987); Hurocy v. Direct Merch. Credit Card Bank, N.A., 371 F. Supp. 2d 1058, 1061 (E.D. Mo. 2005) (denying summary judgment for defendant, which plaintiff alleged had furnished inaccurate information about the plaintiff to credit reporting agencies).

[237] 15 U.S.C. §§ 1681s-2(a), (c)(1), *amended by* Pub. L. No. 108-159, 117 Stat. 1966 (2003).

[238] *Id.* § 1681s-2(d), *amended by* Pub. L. No. 108-159, 117 Stat. 1966 (2003). Courts have upheld this immunity. *See, e.g.*, Nelson v. Chase Manhattan Mortg. Corp., 282 F.3d 1057, 1060 (9th Cir. 2002) (reversing dismissal of claim). *But see* Geeslin v. Nissan Motor Acceptance Corp., No. 1:97CV186-DA, 1998 WL 433932, at *5 (N.D. Miss. June 3, 1988) (denying provider's motion to dismiss § 1681s-2(a) claims against it with no reference to the explicit statutory provision).

[239] 15 U.S.C. § 1681s-2(b)(1); *see also Nelson*, 282 F.3d at 1059-60 (reversing dismissal of consumer's action); Scott v. Amex/Centurion S&T, No. 3:01-CV-1594-H, 2001 WL 1645362, at *6 (N.D. Tex. Dec. 18, 2001) (accepting magistrate's conclusion of law that consumer's complaint be dismissed with prejudice); Thomasson v. Bank One, La., N.A., 137 F. Supp. 2d 721, 723 (E.D. La. 2001) (denying provider's motion to dismiss); Mandly v. Bank One

misattributed an event to an individual, requires furnishers who have received a notice from a consumer reporting agency that a consumer has disputed the completeness or accuracy of consumer data, to investigate the dispute and modify, block, or delete the information if the furnisher cannot verify its accuracy.[240] However, furnishers only become subject to that provision *after* the aggregator has already attributed the bad data to the individual and reported the attribution to a third party. By that point, the consumer has lost dignity and his rightful reputation. That is, the bad data has already been put into the sea of information, from where, given the duplicatability of electronic records, it may be impossible for the consumer to retrieve and remediate it.

2. Preemption of State Laws

The FCRA fails to protect individuals' reputations by allowing providers and aggregators to misattribute information and immunizing them from state action except where a plaintiff can show malice. In addition, it further exposes people to a high risk of digital defamation by preempting many state laws that would otherwise provide an avenue of recourse to those who suffered from an unearned reputation tainted by the deeds of another.

By its express language, the general preemption rule under the Act provides that the Act does *not* preempt state law claims.[241] However, in

---

Dayton, No. 99-1358-PHX-RGS, 2000 U.S. Dist. LEXIS 16269, at *6 (D. Ariz. Sept. 18, 2000) (same); McMillan v. Experian Info. Servs., Inc., 119 F. Supp. 2d 84, 89 (D. Conn. 2000); Dornhecker v. Ameritech Corp., 99 F. Supp. 2d 918, 927 (N.D. Ill. 2000); Ryan v. Trans Union Corp., No. 99-C-216, 2000 WL 110040, at *1 (N.D. Ill. Aug. 4, 2000); Whitesides v. Equifax Credit Info. Servs., Inc., 125 F. Supp. 2d 807, 812-13 (W.D. La. 2000) (denying provider's motion for summary judgment); Johnson v. U.S. Dep't of Defense, No. 99-1699(DWF/AJB), 2000 WL 33956225, at *3 (D. Minn. Oct. 17, 2000); Thompson v. Elec. Transaction Corp., No. 1:98CV305-P-B, 2000 WL 33907674, at *6 (N.D. Miss. Mar. 30, 2000); Olexy v. Interstate Assurance Co., 113 F. Supp. 2d 1045, 1047-48 (S.D. Miss. 2000); Bruce v. First U.S.A. Nat'l Ass'n, 103 F. Supp. 2d 1135, 1142-43 (E.D. Mo. 2000) (denying, in part, provider's motion to dismiss); DiMezza v. First USA Bank, Inc., 103 F. Supp. 2d 1296, 1301 (D.N.M. 2000) (same); Campbell v. Baldwin, 90 F. Supp. 2d 754, 756 (E.D. Tex. 2000) (denying motion to dismiss); Brown v. Maine Med. Ctr., No. 98-444-P-C, 1999 WL 33117137, at *3 (D. Me. Mar. 18, 1999) (magistrate's recommendation to deny motion to dismiss). *But see* Carney v. Experian Info. Solutions, Inc., 57 F. Supp. 2d 496, 501 (W.D. Tenn. 1999) (holding no private cause of action to enforce data provider's reinvestigation responsibilities, using an implausible construction of the provision).

240 15 U.S.C. § 1681s-2(b)(1), *amended by* Pub. L. No. 108-159, 117 Stat. 1954 (2003).

241 *Id.* § 1681t(a) (Supp. III 2003). Section 1681t(a) provides as follows:

> Except as provided in subsections (b) and (c) of this section, this subchapter does not annul, alter, affect, or exempt any person subject to the provisions of this subchapter from complying with the laws of

an example of the exceptions swallowing the rule, the FCRA lists several specific preemption provisions that override any state "requirement or prohibition" bearing a designated degree of similarity to the federal provision, regardless of whether the state law is inconsistent or provides the consumer greater protection.[242] For example, the Act preempts all state requirements or prohibitions relating to the subject matter of all of the responsibilities of data providers to furnish accurate information and to reinvestigate information contested as inaccurate.[243]

As discussed above,[244] the one type of misattribution that Congress directly addressed is that arising from identity theft.[245] However, Congress specifically preempted state laws that address the same conduct as the identity theft provisions of the Act.[246] Thus, the Act drastically limits the ability of states to control how data aggregators and their clients must respond to identity theft.[247]

3. Qualified Immunity from State Common Law Torts

The right to redress for someone's false report of an act has traditionally been in tort, the province of state law. Not only does the FCRA and interpreting case law drain its own effectiveness by voiding many private actions against data providers, it also seeks to sweep away state common law causes of action that protect the dignity and integrity of individuals' reputations. The FCRA limits certain state common law

---

> any State with respect to the collection, distribution, or use of any information on consumers, or for the prevention or mitigation of identity theft, except to the extent that those laws are inconsistent with any provision of this subchapter, and then only to the extent of the inconsistency.

Id. The exceptions in subsections (b) and (c) are discussed below, *infra* notes 242-46.

242 15 U.S.C. § 1681t(b) (Supp. III 2003). Prior to the 2003 revisions to the Act, the then-existing preemption provisions were due to expire on January 1, 2004, 15 U.S.C. § 1681t(d) (2000), and it was that pending expiration that motivated Congress to act not only to enshrine the provisions but greatly expand them. *Id.*; *see also* Hendricks, *supra* note 39, at 337-65 (describing the intense lobbying efforts of the financial services industry).

243 15 U.S.C. § 1681t(b)(1)(F), *amended by* Pub. L. No. 108-159 (2003). However, the Act preserves actions brought pursuant to MASS. GEN. LAWS ch. 93, § 54A(a); and CAL. CIVIL CODE § 1785.25(a), as in effect on the date of enactment of the Consumer Credit Reporting Reform Act of 1996. *Id.*

244 *See supra* text accompanying notes 73-79.

245 *See supra* text accompanying notes 73-79.

246 15 U.S.C. § 1681t(b)(5)(B)-(C), *added by* Pub. L. No. 108-159, § 711, 117 Stat. 1952 (2003).

247 *Id.* § 1681t(b)(5). Among the new duties of agencies that are related to identity theft and that are now preempted are those in sections 1681c-1 (identity theft prevention; fraud alerts and active duty alerts) and 1681c-2 (block of information resulting from identity theft). *Id.*

tort actions by victims of false reports, immunizing data aggregators, users, and providers from any action "in the nature of defamation, invasion of privacy, or negligence" based on information disclosed pursuant to the Act,[248] unless the plaintiff proves that the "false information [was] furnished with malice or willful intent to injure" the plaintiff.[249]

Congress imposed this limitation as a *quid pro quo* for the Act's requirements that agencies disclose to consumers the information that they reported on them.[250] Thus, the qualified immunity provision should not completely shield data providers and aggregators from the designated causes of action. It merely raises the level of proof required of a consumer who brings a defamation, privacy, or negligence action against an agency or a furnisher. Consumers will be more likely to be able to show "malice"[251] than "willful intent to injure."[252] So, what does "malice" mean for purposes of the Act? Courts have largely adopted the same standard issued by the Supreme Court in *New York Times v. Sullivan*, which held that the First Amendment requires a public figure in a defamation action to show that the publisher of a false story published

---

[248] *Id.* § 1681h(e) (2000). The provision in its entirety states as follows:

> **(e) Limitation of liability**
> Except as provided in sections 1681n and 1681o of this title, no consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any consumer reporting agency, any user of information, or any person who furnishes information to a consumer reporting agency, based on information disclosed pursuant to section 1681g, 1681h, or 1681m of this title, or based on information disclosed by a user of a consumer report to or for a consumer against whom the user has taken adverse action, based in whole or in part on the report except as to false information furnished with malice or willful intent to injure such consumer.

Id.

[249] *Id.* The qualified immunity provided by the Act applies only if the consumer discovered the information through a disclosure mandated by the Act. *Id.*

[250] *See Hearings on S. 823 Before Subcomm. on Fin. Insts. of the Senate Banking & Currency Comm.*, 91st Cong. 71 (1969). Senator Proxmire, the bill's primary sponsor, originally intended to preserve traditional state law remedies for false information. *Id.* at 24. However, to assuage industry concerns that the Act's required disclosures would release a barrage of lawsuits against agencies and their furnishers—a fear that perhaps reflected the unease of the industry with the accuracy of its data—Senator Proxmire proposed the limited immunity. *Id.* at 104. Consumer advocates strenuously opposed this bargain. *See also* Thornton v. Equifax, Inc., 619 F.2d 700, 703 (8th Cir. 1980); Yeager v. TRW, Inc., 984 F. Supp. 517, 522 (E.D. Tex. 1997) (noting bargain); Retail Credit Co. v. Dade County, 393 F. Supp. 577, 584 (S.D. Fla. 1975).

[251] *See infra* Part IV.A.

[252] 15 U.S.C. § 1681h(e).

false information with the knowledge that the information is false or with reckless disregard of its truthfulness.[253] To prove reckless disregard, some have stated that the plaintiff must show that the speaker "entertained actual doubt" about the truthfulness of the statement.[254]

As further discussed below, the power of disconnected data on individuals and the capabilities of information technology are such that much misattribution of data arises from just such "reckless disregard" of the truth.[255] That courts have adopted this standard for purposes of the FCRA's qualified immunity provision does not indicate that the standard is required by the Constitution; the Supreme Court made that clear in *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[256] where it held that mere negligence sufficed to impose liability on a consumer reporting agency that published false information.[257]

In short, while appearing to protect consumers, the Act protects those who tarnish consumers' reputations by attributing the acts of another to the consumer. The Act denies those individuals the ability to enforce many of the Act's own accuracy provisions, while at the same time providing qualified immunity from state causes of action that might arise from the agency's mishandling. Simultaneously, the Act wholly bars states from protecting their citizens from much of the damage bad data can do, explicitly claiming a monopoly on much of the territory. The showy substance of the 2003 amendments, which emphasize furnisher responsibility and the consequences of identity theft, may have distracted us from the impotent enforcement powers and the preemption

---

253 376 U.S. 254, 279 (1964). Cases applying this standard include *Cousin v. Trans Union Corp.*, 246 F.3d 359, 376 (5th Cir. 2001) (vacating judgment for the plaintiff); *Rhodes v. Ford Motor Credit Co.*, 951 F.2d 905, 906-07 (8th Cir. 1991) (granting creditor's motion for summary judgment where creditor was merely negligent in falsely reporting that borrower had defaulted on her car loan payments); *Thornton v. Equifax, Inc.*, 619 F.2d 700, 705 (8th Cir. 1980) (citing standard as "an example of a type of malice necessary to overcome a qualified privilege"); *Gordon v. Greenpoint Credit*, 266 F. Supp. 2d 1007, 1012 (S.D. Iowa 2003); *Bruce v. First U.S.A. Bank*, 103 F. Supp. 2d 1135, 1142-43 (E.D. Mo. 2000); *Yeager v. TRW Inc.*, 984 F. Supp. 517 (E.D. Tex. 1997); *Wiggins v. Equifax Servs., Inc.*, 848 F. Supp. 213, 223 (D.D.C. 1993); *Hoglan v. First Sec. Bank of Idaho*, 819 P.2d 100, 102-03 (Idaho 1991).

254 *See, e.g.*, *Bruce*, 103 F. Supp. 2d at 1145 (granting summary judgment to furnisher who had reported a fraudulent account as belonging to the plaintiff); *Wiggins*, 848 F. Supp. at 223.

255 *Bruce*, 103 F. Supp. 2d at 1145.

256 472 U.S. 749 (1985).

257 *Id.* at 795. The FCRA's qualified immunity provision did not raise the plaintiff's level of proof because the plaintiff was a commercial enterprise, and accordingly the Act did not apply to the defendant's report. *See* 15 U.S.C. §§ 1681a(c)-(d) (Supp. III 2003) (defining a consumer report as pertaining to a consumer's eligibility for credit, insurance, employment, and other designated transactions defining a consumer as an individual).

of state laws. Nonetheless, some arenas of traditional relief may still exist, as discussed below.

IV. REVIVING THE COMMON LAW TORT OF DEFAMATION TO PROTECT INDIVIDUALS' REPUTATIONS, PERSONALITIES, AND DIGNITY

When the aggregator- and provider-friendly interpretations of the FCRA's accuracy provisions are paired with the qualified immunity provisions and state law preemption provisions, arguably the Act becomes not a consumer protection act, but rather a data provider and data aggregator protection act. Individuals cannot depend upon the Act to protect their reputations, even though the power of data aggregators to assemble data about (or purportedly about) consumers has swelled, and that data has more power over individuals' lives than ever. State tort law, then, could be a viable alternative. After all, historically, tort law has been the source of remedies for damage done by bad information.[258] Furthermore, defamation, a word that derives from a Latin phrase meaning to spread rumor by false report, far more closely identifies the injury misattribution does to a person's dignity and reputation than does the sterile-sounding "Fair Credit Reporting Act."

The two torts designed to protect reputation are defamation and the privacy tort of false light. Defamation is a communication that "tends so to harm the reputation of another as to lower [that person] in the estimation of the community or to deter third persons from associating or dealing with [that person]."[259] The tort of false light, one of the four privacy torts classified by Dean Prosser,[260] provides redress against one who gives publicity to a matter concerning another that places the other before the public in a false light, if that false light would be highly offensive to a reasonable person, and the publisher either knew that the matter was false or acted in reckless disregard as to the matter's falsity.[261] These torts are the historical avenues of redress for those whose reputations are poisoned by those who misattribute transactions mismatched to individuals. In contrast to the FCRA, they do not offer a free pass to the misattributors. However, as discussed above, the FCRA

---

[258] *See* Sheffer v. Experian Info. Solutions, Inc., No. 02-7407, 2003 U.S. Dist. LEXIS 12728, at *14 (E.D. Pa. July 24, 2003) (denying defendants' motion for summary judgment on credit defamation claim). A false statement in a credit report can be defamatory if it tends to deter others from dealing with the plaintiff. *Id.*

[259] RESTATEMENT (SECOND) OF TORTS § 559 (1977).

[260] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960); *see also* RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977).

[261] RESTATEMENT (SECOND) OF TORTS § 652E.

tries to deter defamed individuals from availing themselves of these torts by offering data aggregators and data providers qualified immunity from them, and overly-expansive readings of that protection has led to the "frothy Chaos" of rumor and gossip clogging databases now. However, an appropriate reading of the qualified immunity provision, one that comports with modern access to and use of technology, could make these torts meaningful tools with which to clean up corrupted data and motivate actors to verify the information that they put into the data sea.

Traditionally, false light has protected a person's right to be let alone, while defamation has protected people's interests in their reputations.[262] But defamation protects not just the reputation of a person, but also the right to dignity by protecting one's interest in being included within the portion of society that is worthy of respect.[263]

Falsely connecting the act of one to the identity of another not only injures the reputation of the one stuck with the act, it violates that person's personhood and injures that person's dignity.[264] A flawed digital image that includes the events not wholly of one's making inflicts the sort of damage to dignity that defamation law seeks to protect.[265] That injury occurs even if the misattributed information is not derogatory. Defamation protects "the *manner* in which the image of the self is constructed in the social realm."[266]

Though the FCRA federalized the law governing credit reports, states continue to have a strong interest in protecting the reputation and dignity of their citizens through common law torts such as defamation, a principle repeatedly affirmed by the Supreme Court. In *Gertz v. Welch*, the Court underscored "the compensation of individuals for the harm inflicted on them by defamatory falsehood" as a "legitimate state interest."[267] Given that interest, the Court "would not lightly require the State to abandon this purpose."[268] The decision quoted the following words of Justice Stewart:

---

262 PROSSER AND KEETON ON TORTS 864 (W. Page Keeton, ed., 5th ed. 1984).
263 *Id.*
264 *See supra* text accompanying notes 155-63.
265 Heyman, *supra* note 16, at 1339.
266 *Id.*
267 Gertz v. Robert Welch, Inc., 418 U.S. 323, 341 (1974).
268 *Id.*

> [T]he individual's right to the protection of his own good name "reflects no more than our basic concept of the essential dignity and worth of every human being—a concept at the root of any decent system of ordered liberty. The protection of private personality, like the protection of life itself, is left primarily to the individual States under the Ninth and Tenth Amendments. But this does not mean that the right is entitled to any less recognition by this Court as a basic of our constitutional system."[269]

Notwithstanding the relevance of both torts, defamation is focused on here because, as a general rule, the tort of false light publicity will not help an individual who has suffered from misattributed information because disclosures among those involved in a financial or personal transaction will generally not meet the tort's publicity element.[270] Furthermore, not every state recognizes a cause of action for false light invasion of privacy—in part because of its very overlap with the tort of defamation.[271] Even under the tort of defamation, however, a defamed consumer must still contend with a common law qualified privilege that benefits those who report financial information of others. Once that is done, however, defamation can impose liability for the initial wrongful reporting of information, which can help motivate the data industry to prevent mismatched information from entering the flow of transmittable data.

---

[269] *Id.* (quoting Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) (Stewart, J., concurring)).

[270] RESTATEMENT (SECOND) OF TORTS § 652D cmt. a. The *Restatement* defines "publicity" as meaning "that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.*; *see, e.g.*, Polin v. Dun & Bradstreet, Inc., 768 F.2d 1204, 1206-07 (10th Cir. 1985) (disclosure of plaintiffs' inaccurate credit report to subscribers did not meet element). However, as electronically-stored information grows increasingly accessible, victims of misattribution may be able to meet this element. *Polin*, 768 F.2d at 1206-07.

[271] *See, e.g.*, Elm Med. Lab., Inc. v. RKO Gen., Inc., 532 N.E.2d 675, 681 (Mass. 1989), *abrogated in part on other grounds by* United Truck Leasing Corp. v. Geltman, 551 N.E.2d 20 (Mass. 1990); Lake v. Wal-Mart Stores, Inc., 582 N.W.2d 231, 235 (Minn. 1998); Sullivan v. Pulitzer Broad. Co., 709 S.W.2d 475, 481 (Mo. 1986) (en banc); Howell v. New York Post, Co., 612 N.E.2d 699, 703 (N.Y. 1993); Renwick v. News & Observer Publ'g Co., 312 S.E.2d 405, 413 (N.C. 1984); Yeager v. Local Union 20, 453 N.E.2d 666, 669-670 (Ohio 1983); Brown v. Pearson, 483 S.E.2d 477, 484 (S.C. Ct. App. 1997); Cain v. Hearst Corp., 878 S.W.2d 577, 579-80 (Tex. 1994); Zinda v. La. Pac. Corp., 440 N.W.2d 548, 555 (Wis. 1989).

A. Defamation's Qualified Privilege and the Existing Construction of Malice

1. The Development of the Privilege, Its Mixed Acceptance, and Its Incorporation into the Fair Credit Reporting Act

Defamation was once a viable tool for those defamed by the earliest forms of data aggregators in the modern age—credit agencies. Nonetheless, those agencies were not strictly liable for false information, nor were they usually even liable for negligence. Rather, the common law allowed them a qualified privilege of malice.[272] In this way, the FCRA did not, at least with respect to this one tort, change the common law dramatically by offering aggregators, providers, and users qualified immunity from defamation.[273] Courts developed the privilege to protect those merchants who did a credit business and who needed to know who in their community paid promptly. To protect this need to share information, communications on the subject are privileged if made in good faith. Therefore, in those states that recognize the privilege, a party whose reputation is injured by such a communication must prove actual malice.[274] Eventually commercial agencies took over the business of aggregating credit information and the privilege followed them.[275]

However, not every jurisdiction hands this shield to credit reporting agencies. Some prefer to protect the reputations of individuals from false information. In a decision that assigned decidedly more weight to the dignity of individuals than to creditors' interests in the information, one court characterized the interests as follows in rejecting a privilege to defame:

> If, therefore, it be immoral to spy and pry into the habits and business of another, and to make false statements

---

[272] *See, e.g.*, Dun & Bradstreet, Inc. v. Nicklaus, 340 F.2d 882, 883-86 (8th Cir. 1965); Hooper-Holmes Bureau, Inc. v. Bunn, 161 F.2d 102, 104 (5th Cir. 1947); Moore v. Beneficial Nat'l Bank USA, 876 F. Supp. 1247, 1257 (M.D. Ala. 1995); Dun & Bradstreet, Inc. v. Robinson, 345 S.W.2d 34, 39 (Ark. 1961); Roemer v. Retail Credit Co., 119 Cal. Rptr. 82 (Ct. App. 1975); Lomas Bank USA v. Flatow, 880 S.W.2d 52, 53-54 (Tex. Ct. App. 1994); *see also* Joel D. Eaton, *The American Law of Defamation through* Gertz v. Robert Welch, Inc. *and Beyond: An Analytical Primer*, 61 VA. L. REV. 1349, 1361-61 (1975) (describing the development of qualified privileges).

[273] *See supra* text accompanying notes 257-70.

[274] *See, e.g.*, McDowell v. Credit Bureaus of Southeast Mo., Inc., 747 S.W.2d 630, 631-32 (Mo. 1998) (agency that had falsely reported that plaintiffs, operators of a home construction business, had filed for bankruptcy were entitled to qualified privilege in libel action brought against it). California has codified the common law privilege at CAL. CIV. CODE § 47(c)(3).

[275] HENDRICKS, *supra* note 39, at 177-79.

> about his character and business respectability, it is also illegal by our statute law. If one makes it his business to pry into the affairs of another in order to coin money for his investigations and information, he must see to it that he communicate nothing that is false. The falsehood of the communication, in print or in writing, maligning in effect the private character and mercantile standing, is itself evidence of malice, legal malice; and unless it be strictly a privileged communication in the performance of a public duty, or a private duty, moral or legal, and then *bona fide* and not "as a cloak for private malice" the right of action and redress by damages are the remedies of the injured.[276]

Another court rejected the privilege not on the basis of morality, but on more practical grounds. In *Hood v. Dun & Bradstreet, Inc.*, the defendant, a credit reporting agency, had misattributed two lawsuits that had been filed against a "David Hood" to the plaintiff, who had the same name.[277] The Fifth Circuit, interpreting Georgia law, rejected the agency's assertion of privilege, relying in part on an empirical study that found no difference in the credit availability in a jurisdiction denying the privilege to one that did.[278]

Florida once recognized such a privilege, but one state court of appeals decided to abolish it.[279] Idaho has also refused to recognize such

---

[276] Johnson v. Bradstreet Co., 77 Ga. 172, 175 (1886) (internal citation omitted). The Georgia Supreme Court later emphatically rejected an opportunity to adopt a qualified privilege for credit reporting agencies:

> We cannot agree to this weighting of the scales against the individual who stands alone facing a commercial Goliath with the power to destroy-not necessarily through malice but perhaps merely from carelessness-his credit rating, commercial advantages, insurance protection and employment, all through the publication of erroneous reports concerning his affairs.

Retail Credit Co. v. Russell, 234 Ga. 765, 770, 218 S.E.2d 54, 58 (1975).

[277] 486 F.2d 25, 27 (5th Cir. 1973). The court rejected the agency's argument that credit reports are of general and public interest, stating that "Irresistible logic and the absence of empirical verification compel this court to conclude that the privilege should not be blindly applied to credit reporting agencies in this case." *Id.* at 32.

[278] *Id.*

[279] Vinson v. Ford Motor Credit Co., 259 So. 2d 768, 771 (Fla. Dist. Ct. App. 1972). That court reasoned as follows:

> Times change and principles of law change with them. "A man's credit in this day and age is one of his most valuable assets and without it, a substantial portion of the American people would be without their homes, washing machines, refrigerators, automobiles,

a privilege, understanding the natural consequences it would have: "If a mercantile agency can safely make false reports about the financial standing and credit of the citizen and destroy his business, it can then take the next step with equal impunity and destroy his reputation, leaving him shorn and helpless."[280] A Massachusetts decision reasoned that a reasonable limit on the privilege is justified because "There is no social utility in reports that are made recklessly or without reasonable grounds. The injury to the subject of the report can be great and the person receiving the report gains nothing."[281]

While these decisions make strong policy arguments against such a privilege, as discussed above, Congress incorporated the privilege into the FCRA.[282] Accordingly, if the damage done to an individual's reputation and dignity arises from a report that falls within the FCRA, the Act will require the individual to show malice or willful intent in order to pursue a cause of action for defamation, even if state law would not accord such latitude to the aggregator.[283] In fact, even where the Act's qualified immunity provision does not apply, the individual will likely have to overcome the common law privilege accorded to aggregators, which also generally requires a heightened standard of misconduct.[284]

Malice, as used in the FCRA and in cases interpreting the qualified privilege,[285] does not mean moral malice, as in a desire to harm others.[286]

> television sets, and other mechanical paraphernalia that are now regarded as necessities of life." The impersonal and unconcerned attitude displayed by business machines as to the impact of their actions upon an individual consumer as here reflected was the catalyst for our National Congress to pass the Fair Credit Reporting Act, which provides protection for consumers from irresponsible credit reporting agencies.

Id. (footnotes and citations omitted).

280 Pac. Packing Co. v. Bradstreet Co., 139 P. 1007, 1010 (Idaho 1914); *see also* W. Union Tel. Co. v. Pritchett, 108 Ga. 411, 34 S.E. 216, 216-17 (Ga. 1899) (rejecting privilege, distinguishing cooperative exchanges of information from mercantile agencies, who make a pecuniary use of the information).

281 *In re* Retailers Commercial Agency, Inc., 174 N.E.2d 376, 380 (Mass. 1961) (holding that mercantile agency lost privilege where it issued two inconsistent reports and where significant derogatory information was "susceptible of precise check").

282 *See supra* Parts III.B.1-B.2.

283 15 U.S.C. § 1681h(e) (2000).

284 *See supra* Part III.B.3.

285 *See supra* text accompanying notes 251-70.

286 *See, e.g.*, Dun & Bradstreet, Inc. v. Nicklaus, 340 F.2d 882, 886 (8th Cir. 1965) (common law privilege); Dun & Bradstreet, Inc. v. Robinson, 345 S.W.2d 34, 39 (Ark. 1961) (common law privilege); Roemer v. Retail Credit Co., 119 Cal. Rptr. 82, 85-87 (Ct. App. 1975)

Rather, statutory and common law malice mean acting "with knowledge that [the information] was false or with reckless disregard of whether it was false or not."[287] Malice has also been defined as making a report without reasonable grounds to do so.[288] A few courts have even constrained the definition of "reckless disregard" to require the plaintiff to show that "'the speaker entertained actual doubt about the truth of the statement.'"[289]

2. The Relationship Between the Standard of Malice and Data Technology

The standard of malice should flex to reflect modern database technology, data aggregators' awareness of errors of misattribution, and the power of information and misinformation over individuals. Practices that may have failed to reach the standard before modern information technology developed might well surpass the standard now. That technology allows us to pull up and compare different pieces of information as if they were books on a desk. The failure to examine records over which one has complete control can meet the standard of malice.[290] It is, in fact, even easier to compare data in a database than to find, for example, conflicting passages between two pieces of printed text—the digital form of the information allows it to be pinpointed immediately.

Doubt should arise where data providers are aware of a tendency to undermatch their transactions to the individuals actually making them or when aggregators are aware that the matching algorithms they use are likely to mismatch some records to the wrong individuals, even if for any single report the aggregator does not entertain doubt as to that specific report. That doubt should arise from the knowledge of the rate

---

(common law privilege); Myshrall v. Key Bank Nat'l Ass'n, 802 A.2d 419, 424-25 (Me. 2002); *see also* Dalton v. Capital Associated Indus., Inc., 257 F.3d 409, 418 (4th Cir. 2001) (interpreting FCRA's punitive damages provision, which requires the plaintiff to show the actor acted willfully).

287 N.Y. Times Co. v. Sullivan, 376 U.S. 254, 280 (1964).

288 *In re* Petition of Retailers Comm. Agency, Inc., 174 N.E.2d 376, 380 (Mass. 1961) (reversing judgment against agency on grounds that agency did not lose privilege through mere negligence).

289 Moore v. Equifax Info. Servs. L.L.C., 333 F. Supp. 2d 1360, 1367 (N.D. Ga. 2004) (citation omitted); *see, e.g.*, Whelan v. Trans Union Credit Reporting Agency, 862 F. Supp. 824, 833 (E.D.N.Y.1994) (citing *New York Times Co. v. Sullivan*); Lomas Bank USA v. Flatow, 880 S.W.2d 52, 53-54 (Tex. Ct. App. 1994).

290 *See* Interstate Transit Lines v. Crane, 100 F.2d 857, 860-62 (10th Cir. 1938) (ruling that employee overcame qualified privilege of employer by showing "indifference" to the employee's interests, and affirming judgment of libel against defendant).

of inaccuracies and by the complaints made to data providers and aggregators by defamed consumers.[291] Furthermore, the rising risks of identity theft—just one form of mismatching—have not been unnoticed by the agencies or, for that matter, by Congress.[292] At least one court has identified the rise in identity theft as sufficient on its own to raise the standard of care that aggregators should use and,[293] as noted above, the FTC received more than 240,000 complaints of identity theft in 2003.[294] The awareness of that risk is particularly visible in the new products that agencies and providers offer and the demand for those products.[295] In the old world of paper records, it would have been reckless for an agency to report a negative item, such as a lawsuit, as being the responsibility of a particular individual when an employee had, sitting on his desk, identifying information that conflicted with that in the item. These databases essentially put all of their information at the fingertips of those who provide and aggregate it. Furthermore, these parties know well the power of information; it is what supports the industry. Accordingly, what might not have been reckless treatment of information many years ago may well rise (or fall) to that standard in the present day, given the ability of data aggregators and providers to aggregate and analyze the data in their warehouses and the power that data has over the lives of individuals.

Other torts adapt to fit advances in knowledge and technology; defamation can as well. For example, a medical malpractice action can arise from a doctor's failure to use a current standard of care, including advances in medical technology, rather than the standard of care appropriate in past generations.[296] Similarly, behavior that may not have once arisen to reckless disregard of the truth can now meet that standard.

---

[291] *See* MISTAKES DO HAPPEN, *supra* note 62, at 4.

[292] *See, e.g.*, *Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use, Before the Sen. Comm. on the Judiciary*, 109th Cong. (Apr. 13, 2005).

[293] Graham v. CSC Credit Servs., 306 F. Supp. 2d 873, 881 (D. Minn. 2004); *see supra* text accompanying notes 126, 184.

[294] *See supra* note 73 (citing *FTC Releases Top 10 Consumer Complaint Categories for 2004*, http://www.ftc.gov/opa/2005/02/top102005.htm (last visited Jan. 14, 2007)).

[295] *See supra* text accompanying notes 28-60.

[296] *See* JOHN J. ELWELL, A MEDICO-LEGAL TREATISE ON MALPRACTICE AND MEDICAL EVIDENCE, COMPRISING THE ELEMENTS OF MEDICAL JURISPRUDENCE 54-56 (1860); *see also* John C. Drapp III, Comment, *The National Standard of Care in Medical Malpractice Actions: Does Small Area Analysis Make It Another Legal Fiction?*, 6 QUINNIPIAC HEALTH L.J. 95, 100-01 (2003) (discussing evolution from "the strict locality standard" that was based on the inability of rural physicians to keep up with advances in the profession, as technological advances allowed physicians to learn of such advances).

3. Modern Analog Interpretations of Malice

Although malice should not require intentional wrongdoing, some decisions have deferred so far to aggregators and providers that they have inadequately considered whether evidence of some lower level of mishandling should lift the FCRA's qualified immunity provision. Interpreting "recklessness" to cover behavior such as ascribing an act to an individual when the ascriber's own data system has conflicting information, publishing information from a source the publisher knows to have been inaccurate previously, or failing to counter the fraud running rampant in the consumer data industry does not expand the original concept of appropriate liability, but rather enforces it.[297] Courts need to apply the recklessness standard in light of modern digital technology, rather than of older, analog processes.

For example, a report should not logically include an account opened before the target individual had even been born. In one case, the defendant acknowledged that it used fuzzy matching to assemble credit reports and did not check the accuracy on records whose identity markers did not quite match the target's.[298] Had the defendant done so, it would perhaps have realized before issuing the report that the record of a bankruptcy by one company whose name was similar to the plaintiff's could not have been the plaintiff's because the plaintiff's incorporation date, the institutional equivalent of a birth date, showed that it did not exist at the time of the bankruptcy.[299] Nonetheless, the court concluded that the agency's deliberate use of fuzzy matching was not reckless and dismissed the plaintiff's defamation claim.[300] In fact, it was not reckless; it was intentional.

Similarly, another court dismissed a defamation claim where a consumer reporting agency had merged records belonging to the plaintiff's son and daughter-in-law into plaintiff's credit report, even though the records did not match the plaintiff's social security number, address, or date of birth, and even though the agency continued to misattribute some of the son's accounts to his father after the father alerted the agency of the errors and provided the agency with his own

---

297 *See, e.g.*, Hood v. Dun & Bradstreet, Inc., 486 F.2d 25, 29 (5th Cir. 1973).

298 County Vanlines, Inc. v. Experian Info. Solutions, Inc., 317 F. Supp. 2d 383, 388 (S.D.N.Y. 2004).

299 *Id.* at 386.

300 *Id.* at 389.

accurate identifying information.[301] Another court found that a creditor did not act recklessly in reporting a loan that the creditor had extended to an identity thief as being the responsibility of one of the plaintiffs, even though the identifying documents used by the thief conflicted in several ways with the data in the plaintiff's credit report, including the date of birth and work history.[302]

These internal conflicts in information within an agency or furnisher's ownership should raise doubts as to accuracy before it is ever attributed to any particular person. However, even should overlooking a conflict fail to be reckless at that point, serious doubts as to accuracy should arise once a consumer notifies an aggregator or a furnisher that a debt reported in the consumer's name is not his. Although a certain percentage of such disputes may be weak attempts to avoid answering for a legitimate debt, the risk that some disputes may be valid should trigger in the reporting figure sufficient doubt to look for additional indicia of accuracy. Nonetheless, the Fifth Circuit, in *Morris v. Equifax Information Services, L.L.C.*,[303] held that an agency did not act recklessly in continuing to falsely report a debt as belonging to the plaintiff, even though the plaintiff had notified the agency of his dispute and yet, according to the plaintiff, the agency "continued to publish the same false information about [the plaintiff] without lifting a finger to determine whether the information was false or not."[304] According to the court, the consumer's notification did not "present 'sufficient evidence . . . that the defendant in fact entertained serious doubts as to the truth of [its] publication.'"[305] If serious doubts do not arise from the conflicts within the agency's or creditor's own system or from a consumer's direct challenge to the information, then the malice standard becomes nearly unattainable

One judge, who reluctantly allowed a claim to go forward, questioned why a business would have been motivated to create false accounts upon the application of an identity thief, accounts that the business could expect would be difficult to collect.[306] However, the

---

301 O'Connor v. Trans Union Corp., No. 97-4633, 1999 U.S. Dist. LEXIS 14917, at **2-3, **21-23 (E.D. Pa. Sept. 28, 1999).

302 Aklagi v. Nationscredit Fin. Servs. Corp., 196 F. Supp. 2d 1186, 1196 (D. Kan. 2002).

303 457 F.3d 460 (5th Cir. 2006) (affirming summary judgment).

304 *Id.* at 471.

305 *Id.* (emphasis & citation omitted).

306 Dornhecker v. Ameritech Corp., 99 F. Supp. 2d 918, 932 (N.D. Ill. 2000) (continuing to report accounts after learning of mismatching error could demonstrate the willfulness necessary for punitive damages under the Act).

court's question reveals a number of misunderstandings about the role of information in the digital world. First, the question should not be whether the merchant intended to create a fraudulent account. The plaintiff should not have to show, in order to claim defamation, that the merchant intended, at the time it opened the account, to open it in the name of someone who had not applied for it. For purposes of showing malice, the question should be, when the merchant reported the account's delinquency to the data aggregators, whether that merchant has serious doubts as to whether the identity of the person that the business designated as responsible for the account actually is, in fact, the person who had opened it. Such doubts could, and should, arise from any mismatch between the identity markers in a credit report the business sought at the time the account was opened, such as date of birth, place of birth, or social security number, and those on the application for service. Such doubts could also arise from past experiences with misattribution, from internal fraud-prevention reviews and procedures, or from other revelations of risk. Furthermore, surely such doubts arise when the misidentified individual notifies the business of its error and provides substantiating identifying information, such as date of birth or address, that distinguishes that individual from the account opener. Continuing to attribute the account to that individual after such events should be considered reckless, thereby malicious, and thus grounds for a defamation action.

Second, the statement ignores that the faulty account is just one in thousands. While a business may not intend to open any one particular account for an impostor, it may well not mind the risk of opening some accounts without sufficiently verifying the applicant's identity if the business perceives the costs of absorbing those losses as reasonable in light of other profits. One assessment of those losses includes the relatively small chance that they will have to pay significant damages to the person to whom they wrongly attributed the information. That chance is artificially small because of the burden imposed on individuals to demonstrate recklessness and because of the shield that the FCRA's dated interpretations of the Act's accuracy and immunity provisions grant them.

Finally, the judge's statement above that a business would not be motivated to create an account in the name of someone who did not open it also assumes that someone who does not owe a debt will not pay it, which overlooks the power of negative financial information in the information age. Given the impact a delinquent account may have on an individual and the relatively weak ability of individuals to clear falsely

attributed data, a business may be able to count on strong-arming the individual to pay the debt incurred by another, profiting off of the consumer's need to proceed with his or her transactional life.

The decision portrays a rigid conception of malice, a conception that soldiers on, impervious to changes in technology, uses of that technology by merchants and data aggregators, and the power of information. Curtailing the standard this way allows aggregators all the benefit of advancing technology with no responsibility to use it for the benefit of the individuals on whom they report.

In contrast, where an aggregator's employee, as opposed to its machine, has records that clearly identify two separate people, reporting one person's record as the other can show reckless disregard for the truth, clearing the Act's qualified immunity malice hurdle.[307] In *Wiggins v. Equifax Services*, the plaintiff's employer fired him after a background check service reported that he had a felony conviction on his record. [308] The employer had provided the service with the plaintiff's first name, last name, middle initial, date of birth, social security number, and address.[309] The service's employee located a felony conviction record of someone with the same first and last names, but a different middle initial and date of birth, and reported that conviction as the plaintiff's.[310] The court refused to dismiss the plaintiff's defamation claim against the service, finding that issuing a report before verifying the conviction could meet the reckless disregard standard.[311] Implicitly, the court found fuzzy matching to be an unreasonable data aggregation technique, at least where a human being observes a conflict between the identity markers in the record and those of the target.

By viewing recklessness in light of computers' abilities to consistently and mechanistically compare data, the risk of liability for defaming an individual would rise. That risk could, and hopefully would, motivate data aggregators to use their information technology to cleanse gossip and rumor from their systems.

---

307 *See* Wiggins v. Equifax Servs., 848 F. Supp. 213, 223 (D.D.C. 1993).
308 *Id.* at 217.
309 *Id.* at 216.
310 *Id.* at 217.
311 *Id.* at 223.

4. Modern Digital Interpretations of the Malice Standard

Other courts have adjusted to the advances in technology, realizing that both data providers and data aggregators should be well aware that data may not belong to whom it appears. Failing to acknowledge that risk, by verifying identities of doers of the deeds they report, surpasses that standard of recklessness. One such decision, *Graham v. CSC Credit Services, Inc.*, illustrates the frustrations of a consumer in the digital age who must cleanse his or her biographical record of someone else's deed.[312] In *Graham*, the plaintiff learned when he applied for a mortgage that an identity thief had opened an account with a creditor in the plaintiff's name and that the defendant, a consumer reporting agency, had reported the thief's account as being the plaintiff's responsibility.[313] The plaintiff disputed the ownership of the debt to the agency and also notified the defendant that two addresses listed in the plaintiff's report—one of which the creditor had supplied—were wrong. Although the agency did delete the two addresses, it insisted that the fraudulent account was the plaintiff's, having sent an automated dispute resolution form to the data provider and supposedly receiving an automated response that verified the account.[314] The agency only deleted the misattributed account when the plaintiff insisted on challenging it for a second time.[315]

This sort of problem might be far rarer if agencies stored not just new items of information, but the sources of that information. Recording sources would reveal information about the item's reliability and could indicate identity theft. In reviewing the plaintiff's claim that the agency had not only violated the FCRA, but had done so willfully, the *Graham* court castigated the agency for designing its database so as not to record the source of data and emphasized that the substantive standard of reasonableness under the Act moves with advances in technology.[316]

Agencies, the court stated, "have a duty to update their systems to continue to strive for accuracy" in the face of "new dangers, such as identity theft."[317] The court noted the FTC's report that millions of

---

312 306 F. Supp. 2d 873, 881 (D. Minn. 2004).

313 *Id.* at 876 n.1.

314 *Id.* The agency insisted that the creditor verified the debt electronically, but the creditor disagreed, stating that it had a note in its files that the account might be fraudulent. *Id.*

315 *Id.* at 877.

316 *Id.* at 883.

317 *Id.* at 881 n.1.

Americans had been victims of identity theft in the recent past.[318] Thus, changes in technology and in information use "change the definition" of what is reasonable.[319] The court held that the agency's "intentional policy decision" to avoid structuring its system to lower the risk of misattributed data could justify punitive damages under the FCRA.[320]

Other courts have also reasoned that to knowingly mismatch or undermatch records can be reckless. For example, in *McMillan v. Experian*, a furnisher reported the account of a son as being that of his father, who had the same name, even after the father challenged it and even though the two had different dates of birth, addresses, phone numbers, and employment addresses.[321] The court ruled that such undermatching could show reckless disregard for the truth and denied the furnisher's motion for summary judgment on the plaintiff's defamation claim.[322] Similarly, in *Stevenson v. Employers Mutual Ass'n*, an employee was suspended from his job after the defendant, who was hired to do background checks, reported that he was a three-time convicted felon after matching the convictions to another by the same name.[323] The court ruled that the defendant's failure to check its match by examining a physical description of the criminal or by comparing the plaintiff's work record to the criminal's times of imprisonment could be sufficiently reckless to pass the FCRA's malice hurdle, and it denied the defendant's motion to dismiss the plaintiff's libel claim.[324]

Even if the original mismatching of a record to an individual is not reckless, once the individual contacts an aggregator or provider about the error, that aggregator's next report of the record should meet the recklessness standard and amount to malice.[325] So, for example, if a business opens an account upon an identity thief's application, the individual to whom the data provider attributes the debt should be able to show malice if the provider continued to report the account in the

---

318 *Id.*

319 *Id.*

320 *Id.* at 881. That is, that the policy decision could constitute a willful violation of the Act. 15 U.S.C. § 1681n (2000). Some decisions equate willfulness with malice. *See, e.g.*, Crane v. Trans Union, L.L.C., 282 F. Supp. 2d 311, 322 (E.D. Pa. 2003).

321 170 F. Supp. 2d 278, 282 (D. Conn. 2001).

322 *Id.* at 287.

323 960 F. Supp. 141, 142 (N.D. Ill. 1997).

324 *Id.*

325 *See, e.g.*, Weir v. Citicorp Nat'l Servs., 435 S.E.2d 864, 867 (S.C. 1993) (affirming trial court's denial of data provider's motion for a directed verdict where plaintiff showed that he had contacted the provider about the account several times yet the provider continued to report the account as his, and stating that the jury could infer malice from such conduct).

individual's name, even after the individual has notified the provider of the theft.[326]

Neither of the Seventh Circuit mismatching cases discussed earlier, in relation to the FCRA's standards, involved defamation claims, and accordingly they did not analyze malice.[327] However, had those decisions used the interpretation advocated here, that aggregators are reckless when they misattribute a transaction to an individual notwithstanding that they have learned that their own databases clearly reveal irresolvable inconsistencies, both plaintiffs would have been able to recover for the damage done to their reputations. In *Crabill*, where the agency wrongly attributed to the plaintiff information belonging to the plaintiff's brother, the attribution was reckless because the identifying information of name, social security number, and date of birth of the two brothers were in such clear conflict.[328] Once the plaintiff notified the agency of the error and specifically requested that the agency put "'do not confuse with brother John D. Crabill'" in every report, the agency's continued misattributions surpassed recklessness, arguably rising to intentional.[329] In *Sarver*, where the aggregator, a consumer reporting agency, attributed accounts that indicated the borrower's bankruptcy to the wrong individual, the agency acted recklessly at the latest when it repeated the misattribution, even after the plaintiff had notified the agency of its error.[330]

In sum, many present day information practices are reckless, and defamation liability likely should arise. The limitations on lawsuits for the false imputation of one doer's event to another should reflect the realities of current or even recently obsolete information technology. As discussed above, the problem of misattributing a particular event to the wrong doer is a problem of mismatching identity. If we think of identity as comprising a collection of Goffman's identity pegs, the increase in the volume of recorded transactions increases the risk that using just one peg—for example a social security number—will mismatch the record to the wrong person. When identity pegs are made fuzzy by identification

---

326 *See, e.g.*, Dornhecker v. Ameritech Corp., 99 F. Supp. 2d 918, 922-23 (N.D. Ill. 2000) (continuing to report accounts after learning of mismatching error could demonstrate the willfulness necessary for punitive damages under the Act); Wiggins v. Equifax Servs., Inc., 848 F. Supp. 213, 223 (D.D.C. 1993) (where an employee of the agency knew that the target of the report had a different middle name and date of birth from that on derogatory record, malice requirement could be met, denying agency's motion for summary judgment).

327 *See supra* text accompanying notes 208-33.

328 259 F.3d 662, 663 (7th Cir. 2000).

329 *Id.*

330 390 F.3d 969, 970 (7th Cir. 2004).

algorithms that deliberately undermatch those pegs, the risk becomes even higher. However, technology can help identify matching errors by checking for anomalies and, when one arises, verifying additional identity pegs to drop the risk of misattribution. Once aware of a risk of misattribution, failing to use information over which one has complete possession and control to maximize accuracy is every bit as reckless under the malice standard as if the contradiction were apparent from the face of two pieces of paper, as in *Wiggins v. Equifax Services*,[331] instead of from two different digital records.

An updated understanding of recklessness, for purposes of tort liability, for mismatching of data could also expand the protections of the FCRA. A practice that was reckless for purposes of defamation law should fail the FCRA's demand that data aggregators use "reasonable procedures to assure maximum possible accuracy"[332] and to reasonably reinvestigate disputes,[333] surely unreasonable for purposes of the FCRA.

Recognizing the culpability of the participants in the data market by characterizing these practices as reckless is justified by several circumstances. First, the problem of misattribution is well known to the data market participants. The volume of consumers' disputes to agencies and of complaints to the FTC has given them notice of the flaws in their data verification practices. Other justifying circumstances are discussed below.

B. Reinterpretation Will Promote Dignity, Personhood, and Liberty

The computer age, the Internet, and the development of information technology have provided people with immense power to impact the social identity of individuals; such power should bring with it inherent responsibility that has not yet been adopted or imposed. As discussed above, by interpreting "recklessness" in light of the immense capacity of modern data technology to analyze and verify data, the common law can provide defamed consumers with an avenue for redress. More importantly, raising a specter of liability for initial false reports would motivate data providers and aggregators to ensure the integrity of data and reports, which would keep false information from falling into the pool of data, from which it is so very hard, maybe impossible, to fully and thoroughly retrieve it.

---

331 *Wiggins*, 848 F. Supp. at 223.

332 15 U.S.C. § 1681e(b) (2000); *see also supra* text accompanying note 184-85.

333 15 U.S.C. § 1681i(a); *see also supra* text accompanying notes 184-85.

Right now, the FCRA and outdated interpretations of its qualified immunity from defamation and of the common law's own privilege have allowed data providers, aggregators, and miners to benefit from the technology that allows them to pull, cull, and analyze immense amounts of data while at the same time receiving protection from interpretations of law that overlook the mastery those aggregators have, or should have, over the data they warehouse. This robs consumers of dignity and personhood by presenting these distorted virtual images as themselves and exposes them to a higher risk of being deemed financially unfit, while maximizing the impact of false information. Existing interpretations effectively allow them to defame until forced to stop.

Primary protection of reputation, personality, and dignity require preventing the injury to begin with. Tort law has always had the motive of preventing injury, and defamation is the age-old tool to protect these interests. In contrast, federal statutory law, like the FCRA, has not traditionally protected personhood. As used and interpreted, it does not prevent injury to personality or reputation, but provides a rather haphazard system of remedies and non-remedies for those who have been injured by the false attribution of a negative act.

Roscoe Pound argued that the right to one's personality develops logically from a Kantian formula of justice that is confirmed by showing that in the evolution of society the right has been increasingly recognized.[334] The protection of personality passes the test of whether it promotes "the general, the public, organization and order, . . . in such a way as to equalize opportunity for all."[335]

Defamation is the method by which society protects dignity, which Robert Post characterizes as the "respect (and self-respect) that arises from full membership in society."[336] The law of defamation enforces "society's interest[s] in its rules of civility."[337] Furthermore, in contrast to the FCRA, where few decisions have found meaningful liability for the initial report of false information, the common law of defamation can impose liability for the original reporting of false information.

Defamation not only serves to protect dignity, it protects that aspect of the right to personality that allows individuals control over how their image is portrayed to the rest of the world. Our capacity to remain

---

334 Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 343, 351-52 (1915).
335 *Id.* at 347 (quoting JOHN DEWEY & JAMES TUFTS, ETHICS 482-83 (1908)).
336 Post, *supra* note 160, at 711.
337 *Id.*

independent from external forces or stimuli is threatened by the irresponsible use of detached data. With the loss of control, an individual loses the ability to determine the image seen by others and the reputation portrayed to others. Daniel Solove, in arguing for privacy protections, argues that they are needed because "concerns about being misjudged and having one's reputations poisoned can make people profoundly unfree, shackling them to their perceptions of how they will be perceived."[338]

That loss of control can, in turn, drive one to internalize the false image.[339] Steven Heyman argues that a person who is denied the right to self-determination is denied liberty.[340] As he notes, the right to personality entitles one to determine "one's own inner life without wrongful interference" from others.[341] False data interferes with this right.[342]

While defamation and invasion of privacy torts such as false light protect the damage to individuals, routine dissemination of bad data can damage dignity in a systemic way, beyond the injury to an individual's "inviolate personality."[343] Lies do not contribute to the "democratic dialogue," but rather "distort[ ] the collective search for truth."[344] One scholar has even insisted that defamation law "is as essential to the health of the [country] and the press as it is to the victims of

---

[338] Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1040 (2003).

[339] *See* Heyman, *supra* note 16.

> Thus there is a certain unity between the self and its image, just as there was between the self and the body in the sphere of external rights. Moreover, the self asserts a claim to its image, for it is only through this image that it is capable of interacting with others and thus fully realizing itself. It follows that one has a right to one's image, including one's reputation. This right has two elements. Negatively, it consists in a right not to have actions or characteristics falsely imputed to oneself. Positively, it is the right not to be deprived of the image that one has legitimately acquired through interaction with others.

Id. at 1338.

[340] *Id.* at 1314.

[341] *Id.* at 1325. Heyman's thesis is that the rights to self-determination and one's personality justifies certain limits on First Amendment freedoms that interfere with such natural rights. *Id.* at 1279, 1333.

[342] *Id.* at 1333-34. Heyman compares defamation to battery and intentional infliction of emotional distress, in terms of the injuries inflicted. *Id.*

[343] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 205 (1890) (arguing for a new tort to protect individuals' privacy).

[344] Melville B. Nimmer, *The Right to Speak from* Times *to* Time: *First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 CAL. L. REV. 935, 951 (1968).

defamation."[345] Justice White, in his dissent from the majority opinion in *Gertz v. Robert Welch, Inc.*,[346] argued that state libel laws arose to protect the "essential dignity and worth of every human being—a concept at the root of any decent system of ordered liberty" and that such laws were necessary for the continued existence of our political system.[347] In order to be able to achieve that protection, given data aggregation and the "frothy Chaos" of errors,[348] defamation and false light torts should be interpreted consistently with the capabilities of those who create, report, and distribute consumer information and with the power of such information to harm individuals.

Furthermore, it is not just the defamed individual who suffers from data pollution; those who rely on that data to make decisions also are harmed. A polluted sea of data will lead to poor business decisions—for example, an employer could lose out on a valuable and profitable employee or a lender could lose out on a trustworthy borrower. If such entities are suffering, then one might reasonably ask why do they not assert their own claims against data aggregators. Perhaps it is because the damage suffered when one deal is lost is slight compared to the total numbers.

One criticism of common law is that it is too reactive and too gradual in its change to effectively protect against the misuse of information technology.[349] A similar criticism of tort law is that it is intended to remedy isolated, individual wrongs, as opposed to systemic problems.[350] Such an approach is "reactive"[351] and treated as a matter of individual

---

345 David A. Anderson, *Is Libel Law Worth Reforming?*, 140 U. PA. L. REV. 487, 490 (1991).

346 418 U.S. 323, 402 (1974) (White, J., dissenting). The majority held that "so long as they do not impose liability without fault, the States may define for themselves the appropriate standard of liability for a publisher or broadcaster of defamatory falsehood injurious to a private individual." *Id.* at 347.

347 *Id.* at 341. Justice White reasoned that while civilized society may justify some exposure of individuals' lives, those individuals do "not bargain for defamatory falsehoods." *Id.* at 402; *see also* Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1564 (2000).

348 Montaigne, *supra* note 2.

349 Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029, 2033 (2001).

350 Solove, *Enforcing Privacy Rights, supra* note 37, at 1232-33. Solove notes the problem of aggregation—how one individual piece of information may not in and of itself be sensitively revealing, but when aggregated with many other such pieces can form what he calls a "'digital biography'" of a person that can form a whole that is greater than the sum of the parts. *Id.* at 1233. Thus, with aggregation we have "the growing use and dissemination of personal information creat[ing] a Kafkaesque world of bureaucracy . . . ." *Id.* at 1234.

351 *Id.* at 1231.

entitlement.[352] However, providing individuals with even one effective tool with which to repair damaged reputations could motivate those in the consumer data industry to curb undermatching and fuzzy matching of data. Just as the aggregation of different points of personal information can be larger than the sum of the points, perhaps the aggregation of individual torts can also have a systemic impact.

Law and economics arguments that privacy is inefficient because it promotes fraud and hampers the exchange of information do not apply where the information is false, and, in fact, privacy would help cleanse the market of fraudulent information.[353] Nonetheless, defamation law by itself will not cure all the problems consumers have with others' acts stuck to their identities, a solution to what Lawrence Lessig calls "the failure of the information market."[354]

One concern is that rigid matching procedures would cause aggregators to fail to link a doer's deed to the doer, an inaccuracy of a different sort. For example, requiring a name to match exactly might exclude those records where an individual omitted a middle initial, or where a clerk mistyped a social security number. However, the damage done to individuals whose histories are blackened by another's acts should outweigh the smaller harm that the biography a user receives is incomplete. The misery of repairing an inaccurate history extends across months and costs victims time, money, and dignity.[355]

The importance of attributing events correctly has risen with the increased use of credit scores. Users themselves may not access the whole biography to make their own independent assessment of the credibility of each record. The use of credit scores means that users—the credit card companies, the mortgage lenders, the department stores—may well receive only a number produced by the underlying information.[356] Thus, that user may not even be able to alert a consumer

---

352 *Id.*

353 *See* RICHARD A. POSNER, OVERCOMING LAW 532-37 (1995); *see also* Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996) (arguing that substantial economic benefits may derive from privacy rights).

354 Lawrence Lessig, *Privacy and Attention Span*, 89 GEO. L.J. 2063, 2071 (2001).

355 One study of 197 identity theft victims revealed that the average time spent by victims to clear their records was 330 hours and that many lost thousands of dollars in lost wages and spent hundreds in out-of-pocket expenses. Identity Theft Resource Center, *Identity Theft: The Aftermath 2004* 13 (Sept. 2004), *available at* http://www.idtheftcenter.org/aftermath2004.pdf. The victims surveyed reported significant emotional impact from the crime that resembled symptoms of Post-Traumatic Stress Disorder. *Id.* at 20-21.

356 *See supra* text accompanying notes 114-54.

as to the particular record attributed to the consumer that lowered the number in a way that costs the plaintiff an opportunity for a loan or a lower interest rate. The increased automation of credit checks has masked the individual items.

In addition to benefiting individuals, a standard that imposed liability for reckless mismatching of records would enhance the integrity of the pool of aggregatable data as a whole. At present, we have a system that not only fails to promote accurate matching, but may in fact discourage those who create data from sufficiently fixing the identity of the doer and assigning sufficient identity markers to the record to keep it stuck to that individual, making sure it would not be prone to attaching to the identity of another. These practices could retard the improvements that data matching technology offers to both those who use data and those whose data is used.

C. The Feasibility of Meeting the Standard

The technology that could improve the accuracy and integrity of personal information already exists. To maintain the shield of the qualified privilege that defamation accords data aggregators, they should be required to use that technology to verify that a negative record does not bear identity markers that are insufficient to pin that item to a particular consumer, or that the item's identity markers do not differ in meaningful ways from those of the target consumer. That businesses and data aggregators are aware of the risks to consumers of mismatching records and that they have the ability to match deeds more exactingly to their doer's identity is shown by the very products that they create and market. They can require matching of more identity markers to avoid the misattribution errors that arise from undermatching. For example, Experian, on its home page, notifies readers of the risks of identity theft.[357] It advertises a product called "Credit Manager" that notifies a consumer by email of "important changes" to a consumer's report.[358] Given that, as discussed above, the agencies do not keep individual files on consumers, but rather gather information on the fly when requested by sending the algorithm trolling through the databases, the product indicates that they are able to seek new information automatically.[359] Trans Union offers a credit monitoring service called True Credit that also sends email notices of changes within 24 hours, and it offers identity

---

[357] Experian Home Page, http://www.experian.com (last visited Jan. 13, 2007).

[358] Credit Manager Home Page, https://www.creditexpert.com/ (last visited Jan. 13, 2007).

[359] *See supra* text accompanying notes 37-93.

theft insurance and fraud resolution services as well.[360] Equifax warns consumers that it could take up to two years to clear your name if you're a victim of identity theft and offers a product called Credit Watch Gold to help consumers prevent the agency from reporting a thief's debts in their names.[361] The fear of being the target of misattributed information has helped the data aggregator, Equifax, take in record revenue in 2004.[362] Its personal solutions business, where it sells its identity theft prevention products, rose dramatically as well.[363]

This sort of "supermatch," if done routinely, could be used to weed out information not meeting the supermatch standard, which would help improve the accuracy of the snapshot of each consumer's financial image. Furthermore, credit scoring algorithms have already been developed that purport to be able to verify identities by matching identity markers.[364] Such feasibility exists outside the traditional credit reporting industry in the modern data aggregation market as well. One of the leading data aggregators, ChoicePoint, even verifies the range of the issue date for a given person's social security number against the associated date of birth.[365]

The products offered show that these data aggregators are highly aware of the prevalence of identity theft and that they have the analytical capacity to discern unusual activity in a particular consumer's name, at least if the consumer is willing to pay for it. Another product, offered by Equifax, indicates that furnishers should be able to verify the identities of those with whom they do business, which would help them reduce mistranscription errors. Equifax offers businesses the automated ability to "[q]uickly and easily authenticate identities online."[366]

---

360 True Credit Home Page, http://www.truecredit.com/ (last visited Jan. 13, 2007).

361 Equifax Personal Solutions Home Page, https://www.econsumer.equifax.co.uk/consumer/uk/sitepage.ehtml?forward=gb_esn_detail (last visited Jan. 13, 2007); *see also* Credit Watch Gold Home Page, https://www.econsumer.equifax.com/consumer/sitepage.ehtml?forward=esn_detail. (last visited Jan. 13, 2007).

362 Ann McDonald, *Market Watch: Equifax's Stock Soars* (2006), http://www.creditcollectionsworld.com/cgi-bin/readstory2.pl?story=20050801CCRQ313.xml.

363 *Id.*

364 Ann McDonald, *High Points for Credit Scoring*, http://www.creditcollectionsworld.com/cg-bin/readstring.pl?story=20050401CCR0247.xml (last visited Jan. 13, 2007). Each of the big three credit reporting agencies, Trans Union, Experian, and Equifax, uses scoring algorithms to prevent fraud, target collection efforts, and assess risk. *Id.*

365 CHOICEPOINT, PROCHECK: CHOICEPOINT AUTHENTICATION SOLUTIONS 2 (2005), http://www.choicepoint.com/authentication/common/pdfs/ProCheck.pdf.

366 Equifax Business Solutions Home Page, www.equifax.com/biz/solutions/fraud.shtml (last visited Jan. 13, 2007).

V. CONCLUSION

Information about individual transactions that used to just simply evaporate at the conclusion of the deal can now be recorded, searched, analyzed, and passed around, easily accessible once networked into the Internet. At the same time, we are often so detached from our information that a cache of records in a database and not personal knowledge determines whether any particular event is attributed to an individual. Because of the volume of transactions and the need to identify each transaction with a specific flesh-and-blood person, it has become all too easy for a potentially crippling record about a transaction to become ascribed to someone other than the original doer.

Once upon a time, the tort of defamation could provide redress for someone falsely accused of being unworthy of credit, and that redress likely curbed such accusers. Later, the FCRA largely supplanted the old common law action, at least for those financial transactions that fell within its scope. However, those standards impose meaningful requirements on data providers and data aggregators only *after* an item has been wrongly ascribed to an innocent consumer. Furthermore, the Act unreasonably protects data providers and aggregators through its provisions that grant those parties qualified immunity from some torts, provide unqualified immunity from private suit for many of its accuracy standards, and preempt state accuracy standards. This protection is unreasonable because a false attribution may well stick to the consumer even after the consumer has used the Act's provisions to accuse a provider or aggregator of failing to ensure accuracy because digital data is so easily duplicated and transmitted. Once accused, a consumer may never fully restore the reputation arising from those records.

Accordingly, while the Act may have been appropriate for analog records, which were burdensome to search and highly subject to human error. Now, however, bad data has more power and information technology allows those who traffic in data to use computers to analyze, verify, and cross-check it. This mastery over data, in light of the power of that data, justifies meaningful liability for mismatching denigrating information to an individual when the data provider or aggregator could have easily avoided the misattribution. By acknowledging the power providers and aggregators have over the information, the providers' and aggregators' culpability can rise to the level of recklessness necessary to overcome the common law's qualified privilege and the FCRA's qualified immunity from defamation. If the risk of liability for initial reporting rises, data providers and aggregators could direct information

technology to prevent the pollution of the data sea with mismatched information from the start.

Preventing pollution by inaccurate data will help individuals maintain the reputations that they have earned through their own deeds, rather than the deeds of someone else. Their transactional biographies will reflect their own choices and personalities as expressed through those choices. By curbing the reckless use and abuse of information, the common law of defamation can protect the rights of individuals to personal dignity by treating them as individuals who make distinct choices as opposed to objects who serve the purposes of others.