UIC John Marshall Journal of Information Technology & Privacy Law

Volume 26
Issue 1 *Journal of Computer & Information Law - Fall 2008*
Article 2

Fall 2008

Beyond Whiffle-Ball Bats: Addressing Identity Crime in an Information Economy, 26 J. Marshall J. Computer & Info. L. 47 (2008)

Erin Kenneally

Jon Stanley

BEYOND WHIFFLE-BALL BATS: ADDRESSING IDENTITY CRIME IN AN INFORMATION ECONOMY

ERIN KENNEALLY & JON STANLEY*

I. INTRODUCTION

Information technology has enabled Americans to live significant aspects of their lives in a digital environment. The U.S. legal system's response to this shift has been protracted, confused, and uninspired at times. A significant consequence of this muddled response has been a widening gap between a citizen's expectations of a safe and secure digital environment and the stark reality of a chaotic and at times, dangerous, digital environment, mediated by various marketing and advertising perception machines.[1]

The situation resembles one where business and government, racing to exploit the new opportunities that technology inspires, set up a shopping mall to entice visitors. At the same time and unknown to the con-

* Erin Kenneally is a licensed attorney and forensic scientist who consults, researches, publishes, and speaks on prevailing and forthcoming issues at the crossroads of information technology and the law. These include evidentiary, privacy, and policy implications related to information forensics, information security, privacy technology and information risk. Ms. Kenneally is founder and CEO of Elchemy, Inc.and holds a Cyber Forensics Analyst position at the University of California San Diego. Ms. Kenneally holds Juris Doctorate and Master of Forensic Sciences degrees. Jon Stanley is the Director of Tech Law for Elchemy, Inc. and Principal of the Law Firm of Jon Stanley. His focus areas include regulatory concerns for business entities, information security, privacy, cybercrime, cyberspace insurance, and intellectual property, about which he has spoken at various national conferences including the American Bar Association, Computer Security Institute and the Annual RSA Conference. Mr. Stanley earned his J.D. from the University of Maine Law School and his LL.M. in Information Technology and Telecommunications Law from Strathclyde Law School, UK.

This project was supported by Award No. 2005-IJ-CX-K061 and 2006-DE-BX-K001 awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication/program/exhibition are those of the author(s) and do not necessarily reflect the views of the Department of Justice.

1. *See* WordNet, http://wordnet.princeton.edu/perl/webwn?s=chaotic (last visited Aug. 12, 2008) (search definition of "chaotic:" "lacking a visible order or organization").

sumer, this "mall" is a zone where each beleaguered consumer is largely left to his own devices to protect himself from fraud or theft.[2] While the legal system does not allow the outright bludgeoning of harried citizen-consumers in these malls, it implicitly demands a threshold of a near-mugging before it will intervene on the citizens' behalf. Moreover, consumers' choices are increasingly limited to these "unprotected" malls as institutions raze their concrete stores and migrate to the virtual stores.

This would be an untenable scenario in the physical world, yet it is suggested that this is happening in the digital world. This tension between consumer expectations and reality can be viewed as a macro reflection of the features-versus-security tradeoff in software development, where the longstanding and dominant first-to-market policy has not coincidentally spawned demand for more secure code. Yet in this larger digital mall space the outcry for security is dispersed and muffled, thus allowing institutions to continue to drive consumers towards digital transactions without a corresponding investment in the security that would be required in the "physical" marketplace. This paper will explore the underpinnings and state of these pernicious dynamics in the context of identity crime, suggest likely consequences if nothing is done to alter the dynamics, and offer some solutions to bring a more well-founded sense of stability, safety, and order to this emerging and chaotic digital world.

In the throes of an accelerated period of change, society is struggling to make rational choices that strike a balance between traditional consumer expectations about safety and the grim realities of fraud and theft that the consumer faces online. The fear, uncertainty and doubt surrounding personal information privacy are the primary manifestations of this dynamic. The most tangible instantiation of this privacy fear[3] has arguably been the explosion in both alleged and actual Identity Theft Crime("IDC").[4] IDC exposes the rift between citizens' expectations of stability and security, and the reality of society's information age institutions' management of digital data. This paper attempts to drive a proverbial zamboni across the dialogue about the identity theft problem

2. In the digital world these "devices" include, for example, improperly configured firewalls, continuous software patch updates, and anti-virus/malware/spam software.

3. *See* Press Release, TRUSTe, TRUSTe Report Reveals Consumer Awareness and Attitudes about Behavioral Targeting (Mar. 26, 2008), *available at* http://www.truste.org/about/press_release/03_26_08.php.

4. *See* U.S. Dept. of Justice, http://www.usdoj.gov/criminal/fraud/websites/idtheft.html (last visited Aug. 27, 2008). For our purposes here, and throughout the paper the term Identity Theft Crime ("IDC") means: "Identity theft and identity fraud are terms used to refer to all types of crime [or tort violations] in which someone [or some entity] wrongfully obtains and uses or intends to use another person's personal data [or identifying information and/or symbols] in some way that involves fraud or deception, typically [but not exclusively] for economic gain."

rather than taking yet another swing at this complex topic with a whiffle-ball bat. We will highlight the compartmentalized and imbalanced role that the free market and law enforcement plays in response to this emerging threat to privacy, the implications of this dynamic, and recommendations for improving the societal risk management of Identity Crime.

A. The Questions That Will Define the Answers

Fundamental questions that must be addressed in any analysis of IDC include: What is identity in the analog world? What is identity in a digital environment? How is identity unlawfully acquired and used? How and when does this dynamic invoke legal protections? How are and should these legal protections be measured in terms of recoverable loss and/or damages? What is the nature and scope of IDC, and consequently, where are the risk allocation points during the lifecycle of IDC where responsibility and liability for prevention, detection and response should attach? This paper is motivated in part by what the authors contend to be a lack of satisfactory, objective answers to these questions. While this paper does not answer the totality of these questions it exposes the shortcomings of the predominant discourse about IDC, which is often as superficial as the perceptions it ingrains. In so doing, the goal is to direct solution-focused dialogue on these critical issues by providing a deeper and more comprehensive understanding of the role of key institutional forces on the structure and functions of IDC.

An examination starts with the contention that that the relationships between citizens and their institutions are undergoing, at minimum, two significant role transformations in the digital environment.[5] Specifically, we dissect the IDC crisis[6] as owing to the dominion of unregulated or misguided free market forces.[7] It is further suggested that these misguided, or unbounded, free market forces are forging and man-

5. By this term we mean any environment where digital information, information using a series of ones and zeros, is stored.

6. *See* Press Release, Federal Trade Commission, FTC Testifies on Identity Theft (July 12, 2000), *available at* http://www.ftc.gov/opa/2000/07/identity.shtm. Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection, delivered the agency's testimony before the Subcommittee on Technology, Terrorism and Government Information of the Senate Judiciary Committee, stating "The fear of identity theft has gripped the public as few consumer issues have," the testimony says. "Consumers fear the potential financial loss from someone's criminal use of their identity to obtain loans or open utility accounts. They also fear the long lasting impact on their lives that results from the denial of a mortgage, employment, credit, or an apartment lease when credit reports are littered with the fraudulently incurred debts of an identity thief." *Id.*

7. *See* Investorwords.com, http://www.investorwords.com/2086/free_market.html (last visited Aug. 27, 2008) (defining "free market" as "Business governed by the laws of supply and demand, not restrained by government interference, regulation or subsidy.").

aging people's digital personas.[8] Secondly, we posit that law enforcement's ("LE") role in maintaining order in the digital environment is a crippled or greatly diminished version of the role it plays in the physical environment, also exacerbating the IDC problems.

In the physical realm, Western society's traditional guarantor against chaos and corruption has been the legal system, with LE tasked to convey and enforce social protections manifested by laws.[9] Implicit underpinnings of these protections and assurances are Identification[10] and Authentication.[11] Few laws can be enforced or accountability effectuated if violators and victims cannot be credibly identified. Likewise, credit-based commerce depends upon distinguishing between bona fide "transactors" and impersonators, in other words, citizen-consumers and identity criminals.[12]

This two-step process of identification and authentication has been internalized and taken for granted in the physical realm, both by society in general and LE specifically.[13] In the physical realm a person's offline identities are relatively fixed and directly perceived through one's senses, and one's institutional controls, processes, and cultural conventions to authenticate identity have been built around these features.[14] Yet the nature of the digital realm renders people anonymous by default. This is because a person's "online" identity is highly mediated (people experience each other through various hardware and software inter-

8. *See* Roger Clarke, *The Digital Persona and Its Application to Digital Surveillance*, 10 INFO. SOCIETY 25 (1994), *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/DigPersona.html ("The digital persona is a model of the individual established through the collection, storage and analysis of data [and information] about that person. It is a very useful and even necessary concept for developing an understanding of the behavior of the new, networked world.").

9. In contrast to federal LE, local LE is tasked to handle frontline criminal law enforcement.

10. *See* The Free Dictionary, *identity,* http://www.thefreedictionary.com/+Identity+ (last visited Aug. 27, 2008) (defining "identity" as "the collective aspect of the set of characteristics by which a thing is definitively recognizable or known").

11. *See* Wikipedia, *Authentication*, http://en.wikipedia.org/wiki/Authentication ("from Greek *αυθεντικός*; real or genuine, from *authentes;* author is the act of establishing or confirming something (or someone) as authentic, that is, that claims made by or about the thing are true.") (as of Mar. 17, 2009, 15:56 GMT). Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity. *Id.*

12. Charles M. Kahn & William Roberds, *Credit and Identity Theft*, 55 J. MONETARY ECON. 251 (2008).

13. We are by no means unaware that identity abuse happens in the physical/corporeal world. Rather we argue that it is much more efficient and thus scalable in the digital environment, thus making the difference with distinction worthy of special attention.

14. For instance, in a court of law, a witness might authenticate that the Defendant, Tyler Durden, was the person who punched the victim by testifying that he saw the event occur and by pointing to Durden in the courtroom.

faces, and data encoding and formatting), non-fixed (a person's identity attributes are dynamic across time and easy to change) and referential (digital identifiers do not stand-alone, but are defined by reference to the physical person).[15]

Consequently, digital identification and authentication has proved a challenging matter.[16] This is especially so for an institutional control like LE whose viability is largely predicated on being able to identify and authenticate persons, and whose responsibility has been sidestepped or outright rejected as society migrates to the digital environment. In addition, this rejection of the traditional system for establishing or verifying identity and maintaining order has been an amalgamation of unwitting and subconscious decisions, deliberate myopia, and intentional abandonment by those very entities charged with this mandate.[17] Consequently, this has facilitated the online equivalent of *Beyond Thunderdome*,[18] an environment hallmarked by renegade justice where denizens are largely left to fend for themselves in the absence of social or other institutional protection.

The institutional control that has filled this gap is the free market, and more specifically, the financial institutions, credit bureaus, credit card companies, and data brokers influencing economic policy as well as companies willing to accede to and exploit the resulting environment.[19]

---

15. *See* Arthur Allison et al., *Digital Identity Matters* (Aug. 2003) (unpublished article), *available at* https://dspace.gla.ac.uk/bitstream/1905/315/1/digiident-all.pdf. Also, anonymity is inherent to the structure and function of the Internet, i.e., the Internet protocol is not built to correspond to a particular person's identity. While each device attached to the Net has a specific address, this address and users of the device can and does change, and even in situations where a fixed address is associated with a fixed device and coupled to a specific user account, it is common knowledge that any number of individuals can be behind the keyboard and/or user account.

16. Hence the resonance of the cliché, "on the Internet they don't know you're a dog."

17. *See* Susan W. Brenner, *Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMPUTER & TECH. L.J. (2004), *available at* http://pegasus.rutgers.edu/~rctlj/.

18. MAD MAX BEYOND THUNDERDOME (Kennedy Miller Productions 1985). We chose to depart from the oft-cited and antiquated reference to the Wild West, coined by John Perry Barlow in *The Economy of Ideas*. John Perry Barlow, *The Economy of Ideas*, WIRED, Mar. 1994, *available at* http://www.wired.com/wired/archive/2.03/economy.ideas.html.

19. The Organization for Economic Co-operation and Development defines *free market* as:

> A free market economy is one where scarcities are resolved through changes in relative prices rather than through regulation. If a commodity is in short supply relative to the number of people who want to buy it, its price will rise, producers and sellers will make higher profits and production will tend to rise to meet the excess demand. If the available supply of a commodity is in a glut situation, the price will tend to fall, thereby attracting additional buyers and discouraging producers and sellers from entering the market. In a free market, buyers and sellers come together voluntarily to decide on what products to produce and sell and buy, and how resources such as labour and capital should be used.

What people are currently experiencing is the preliminary consequence of the privatizing and outsourcing of their digital identities –the digital personae[20] and its component artifacts– to the free market. This is in contrast to how people's carbon-based personae and its component artifacts[21] have heretofore been defined; recorded and issued by the government directly via law, policies, and regulations and indirectly by the social norms and expectations that evolve from these mechanisms. Instead, free market forces, often bereft of regulation, are defining people's digital personae using code, the brainstem and language of technology, as its handmaiden.

The use of code to implement policy is not undesirable. It is prudent and necessary in the context of an IT society. The critical question is not whether code is the mechanism by which identity is established. Rather the question is: what is the underlying policy that is promulgated via code? Code that is informed by policy and intended to address the security and well being of citizens is desirable. But code, driven by free market policy (i.e., maximization of wealth for corporate owners and managers), risks the creation of an environment where personal identity is treated simply as a commodity. As a result of this latter dynamic, citizens are at risk of being placed in a grossly unequal bargaining position from which to exercise control over their personhood.

This control includes establishing and maintaining integrity in one's digital persona. At present, there is a conflict between the values embedded in the free market use of technology and the values catalyzing the public policy debate regarding digital identity management.[22] What has resulted is a dichotomy between the use of technology to facilitate a free market policy that thrives on the free flow of personal information where our digital identities are the "goods," and the use of technology to safe-

---

The Organization for Economic Co-operation and Development, Free Market, http://stats.oecd.org/glossary/detail.asp?ID=6264 (last visited Apr. 11, 2009). The authors acknowledge that usage of this term in such a broad sense threatens to encompass so many entities as to be rendered meaningless in the context of criticisms and recommendations contained herein. However, we believe that both the relevant entities and policies can be distinguished for purposes of advancing the dialogue advocated herein).

20. *Supra* note 8.

21. *See* Merriam-Webster Online Dictionary, *artifact*, http://www.merriam-webster.com/dictionary/artifact (last visited Apr. 11, 2009) (defining "artifact" as "something created by humans usually for a practical purpose"). This is the definition we intend when we employ the term "traditional artifacts" in this paper. Specifically we mean, among other things, social security numbers, birth certificates, driver's license, passports, and such, as well as fingerprints).

22. Broadly speaking, DIM refers to technologies, methodologies and policies around the creation, authentication, verification, security, and revocation of identity in the digital environment.

guard identity information and allow individuals some control over the integrity of his or her digital persona, respectively.

This pernicious dynamic was captured by Henry A. Valetk in his law review article, *Mastering the Dark Arts of Cyberspace:*[23]

> For too long, the Internet and global policy have evolved at starkly different paces. On the one hand, communications and software development companies [and now, governments] cave to market forces in a rush to introduce new product features [as well as new services] and woo anxious investors. On the other, policymakers put off enacting any legislative proposals that may impose additional administrative burdens so as to not upset their corporate constituents. This crippling imbalance has created an enormous gulf between user expectations and technology's true potential. Consumers remain too vulnerable in cyberspace, and often hesitate[24] before experimenting with the Internet's untapped potential to reach a global audience.

The "imbalance" Valetk refers to has created a predicament for citizens who engage willingly or by necessity in the digital environment. The "vulnerability" has evolved into the social issue *du jour* –ID crime,[25] which owes its existence to the availability, value and disproportionate protection of personal data by the free market, and in some cases, the government.

B. Unraveling the Puzzle Palace

American citizens are increasingly aware of this emerging threat as they are barraged by seemingly endless reports of database thefts and the subsequent fear of IDC they rightly raise.[26] Citizens are newly aware that the unlawful or wrongful acquisition of identity artifacts, whether traditional or digital, is not only widespread and pronounced, but a means to a criminal or otherwise wrongful end.[27] That "end" is the misuse of those personal identifiers and possible corruption of one's digital persona. This is significant as the bulk of people's affairs are migrat-

---

23. Henry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, Stan. Tech. L. Rev. 2 (2004), *available at* http://stlr.stanford.edu/STLR/Articles/04_STLR_2.

24. In fact there is a growing debate as to whether or not consumers are "waiting" or whether they are ignorant of the risks. Nonetheless, citizens' dependence on the services of business and government leaves little opportunity for choosing whether to engage in the digital environment.

25. We have seen other iterations of this crisis: worm/ virus crisis, the spam crisis, the interoperability crisis.

26. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Aug. 12, 2008).

27. *See* Privacy Rights Clearinghouse, Public Attitudes About the Privacy of Information, http://www.privacyrights.org/ar/invasion.htm (last visited Aug. 12, 2008).

ing to the digital landscape and the digital persona is becoming the sole means of interfacing with it.

Are we at a crisis point with our digital personae, and if so, how did we arrive here? What has society's initial reaction been to this crisis? What should society's response be? This work will provide a conceptual framework for understanding and addressing these questions in the following three sections.

Section I defines the problem by dissecting core concepts of "identity" and "authenticity", and the issues surrounding the definition, statistics and analyses of IDC. Section II addresses the current, general state of digital security and related cybercrime, paying particular attention to the relationship between information security and free market forces. This examination exposes the radically shifting role and rising monetary value of personal identifying information (PII), and how this rapid evolution is having a profound effect on the digital persona as reflected in IDC. Included in this section is an assessment of the legislature's historical role in addressing digital security and privacy issues, including the direct and indirect effects and implications of its policy decisions on the creation and protection of the digital persona. Furthermore, Section B will briefly analyze how the judiciary has wrestled with IDC, and its most recognized derivate, ID theft, in both the database breach and civil contexts. In doing so, this section contends that current jurisprudence has disincentivized digital security for data holders, essentially turned its back on the victims of data breaches and IDC, and is contributing to a growing chaotic digital environment.

The examination culminates in Section III which underscores and synthesizes the role of LE in ID theft ("IDT") issues. This final section focuses on how LE can play a vital and fundamental role in understanding the nature, scope and extent of the identity crimes that embroil society. In doing so, this section examines the current role LE plays in addressing unlawful activity, ID crime in particular. Based on this assessment that LE's role is largely passive, disorganized, and underresourced,[28] this section conjectures what the future holds if this dynamic continues. Lastly, this section will offer recommendations for a significant change in policy and procedure to better enable LE to advance its value and capabilities in addressing identity crime.

28. This includes both a shortage of funding and inadequate training, which most certainly correlates with the relative passivity and disorganization.

II. DEFINING THE PROBLEM

A. Identity and Authenticity in Cyberspace –Who Issues and Stamps the "Passport"?

More robust responses to the opening questions are developed by coming to terms with core concepts: identity and authenticity in the digital environment. First, agreeing that digital objects have different properties than physical objects (i.e., my carbon-based person is not the same as my digital person) identity in the digital environment is based on *assertions* of one's physical identity. These assertions are the "digital persona" –the individualizing, socially-meaningful attributes of personal identities upon which individuals and entities assess who they are dealing with in the digital environment.[29]

The digital persona is a set of attributes –such as real name, physical address, telephone number, username and password, PIN, account number, IP address, birth date, Social Security Number ("SSN"), passport number, behavioral patterns, and biometric information –that form one's expectations of the physical entity behind the digital transaction or communication, and upon which digital communication and transactional decisions are based.[30] The meaning of digital persona is evolving piecemeal and oftentimes unconsciously or implicitly by legislation, regulation, jurisprudence, business practices, and cultural expectations. Similar to identity in real space, digital identity attributes are the progeny of the confluence of the law, information technology, and social institutions and norms, all vehicles that control relationships between people, organizations and objects. Therefore, a crime against identity necessarily indicates discordance between these controls that define persons. As such, IDC is a manifestation of the conflict between the free market policies and public good policies embedded in the uses of IT to manage digital identity.[31]

The second core concept upon which to address the problem of IDC is authenticity. To back into this understanding, the more familiar notion of credibility must be the starting point. Credibility in one's digital environment –the corpus of one's electronic transactions, communications and other relationships– hinges on the establishment of a trustworthy digital persona, which in turn is predicated on reliable, digital, artifacts.

---

29. *See* Stan Karas, *Privacy, Identity, & Databases*, 52 Am. U. L. Rev. 393 (2002) (discussing how assertions gain value if their compromise leads to damages to any of the parties involved- the subject and others involved, the parties consuming/relying on the data, or the parties vouching for).

30. In comparison, our offline identity is manifest by physical appearance, behavior and location attributes which we rely on our senses and perceptions, and institutional assertions to distinguish between persons.

31. Note that policies are a reflection of underlying values.

Technology-based credit systems and commercial transactions and services between and among persons and organizations depend on reliable information, of which trustworthy personae and artifacts are a major part.[32] To the extent that artifacts lack authenticity, the greater the risk that social and legal fictions will be created to maintain the perception of trust and stability.

A fundamental characteristic of a trustworthy[33] digital persona is authenticity[34] –the provable link between the identifiers comprising the digital persona and the physical persona.[35] The information comprising the digital persona is that which is expressive and exploitative of identity, and its authenticity is the degree of correspondence to one's carbon-based being.[36] So while persons may have multiple digital personas, authenticity is an objective reference to which any number of digital personae can attach. In turn, relationships that form within this digital environment are based on assertions about these personas, and more importantly, on presumptions and expectations about their trustworthiness. These relationships are commercial, personal and/or purely utilitarian in nature.[37] The more authentic the persona, the more the

32. Personal and business transactions and communications are more frequently occurring across open networks within the larger Internet, oftentimes involving no prior, established physical world relationships.

33. *See* Ann Keith, *Trends in Identity Theft*, *Future Trends in State Courts* (2005), *available at* http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/criminal&CISOPTR=175; Phillip Hunt & Prateek Mishra, *Oracle Identity Governance Framework* (2006), *available at* http://www.oracle.com/technology/tech/standards/idm/igf/pdf/IGF-Overview-02.pdf. Trust is not a binary characteristic, but rather, is tunable. *Id.* The level of trust with which an identifier refers to a specific person may vary based on the purpose of the transaction/communication/relationship. *Id.*

34. *See* Merriam-Webster Online Dictionary, *authentic*, http://www.merriam-webster.com/dictionary/authentic (last visited Apr. 11, 2009) (stating that "authentic implies being fully trustworthy as according with fact. . .[and] it can also stress painstaking or faithful imitation of an original").

35. Some may posit that the digital persona and the physical persona are just different contexts of "identity." We use physical identity as the referential, foundational identity because it is the context around which society has structured its norms, laws and relationships.

36. *See* Matthew D. Ford, *Identity Authentication and "E-Commerce"*, 3 J. INFO. LAW AND TECH. (1998), *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/ford/ ("Identity authentication is the process whereby some chosen attribute of a real-world entity ("the distinguishing character or personality of an individual") is demonstrated to belong to that entity."). It is based on one/more of the following principles: something the claimant knows; something the claimant owns; something the claimant is; and may include that the claimant is at a particular place at a particular time. *Id.* Common identity authentication systems include passwords, physical tokens, biometrics and digital signatures. *Id.*

37. For instance, interactions with the government.

relationship is predictable, beneficial, and the risk of deception is minimized.

Conversely, the more dubious the persona, the greater the risk of deception, accompanied by an inefficient avoidance of risk. A digital environment wrought with heightened risk will inevitably result in some degree of uncertainty, contempt for social institutions, corruption and counter-productivity.[38]

B. Understanding the Scope and Prevalence of ID Theft: Tacking Jell-O to a Wall

It was previously suggested that society's perceptions about the IDC crisis flow from its knowledge and beliefs on the subject matter. This section will begin examining the "facts'" and the societal dialogue which give rise to the knowledge and beliefs about IDC which society is internalizing and/or taking for granted.

The confusions surrounding the definitions, statistics and tracking/analyses of IDC have converged to make understanding the nature and scope of the problem arduous at best. There is no shortage of media accounts highlighting the IDC problem, not the least of which are the satirical primetime television ads that anthropomorphize identity data muggings.[39] IDC self-help tips abound, and a telltale indicator that the issue has hit primetime is the fact that the market now offers identity theft protection services and insurance policies.[40] Yet these are secondary symptoms rather than first source evidence of the IDC problem. The real indicator is what underlies these surface warnings for only here can one begin to understand the scope, extent and dynamics of IDC.

Society lacks objective, reliable, and comprehensive statistics on cybercrime in general, and IDC in particular. This truth raises questions about the validity of the underlying "knowledge and facts" about IDC. Take, for example, some notes of caution presented in the General Ac-

38. Deception is defined here as the exploitation of cognitive assumptions.

39. *See* Citibank Identity Theft Commercials, http://www.identitytheftsecrets.com/videos/citibank_identity_theft_commercial.html (last visited Aug. 13, 2008). In 2007-2008 Citibank ran a series of humorous television advertisements that uniquely personalized the IDT problem. *Id.* In the ads, identity thieves speak through their victims in an overdubbed voice track, and describe their illicit purchases. *Id.* The humor comes from the dissonance between the personae of the victim and the thief.

40. *See, e.g.,* CNA NetProtect, http://www.cna.com/portal/site/cna/menuitem.489f2511a757a1a1df88e0f2a86631a0/?vgnextoid=2c9f65683c2fe010VgnVCM1000008f66130aRCRD (last visited Aug. 15, 2008); AIG netAdvantage, http://www.aig.com/Network-Security-and-Privacy-Insurance-(AIG-netAdvantage)_20_2141.html (last visited Aug. 15, 2008); LifeLock, http://www.lifelock.com (last visited Aug. 15, 2008); Debix, http://www.debix.com/ (last visited Aug. 15, 2008); TrustedID, https://www.trustedid.com/ (last visited Aug. 15, 2008).

counting Office's ("GAO") initial, groundbreaking 1998 report on IDC:[41]

- "Identity fraud is difficult to track because there is no standardized definition."
- "Generally, the law enforcement officials we contacted told us that their respective agencies historically have not tracked identity fraud."
- "We found no comprehensive statistics on the prevalence of identity fraud. . ."

In 2005 the Department of Justice, engaged two experienced criminologists to prepare the document, one of the most comprehensive literature reviews ever done on identity theft.[42] The purpose of the work was to, "[review] available scientific studies and a variety of other sources to assess what we know about identity theft and what might be done to further the research base of identity theft."[43] Here are a few of the conclusions from the 2005 Review:

- "This paper departs from the usual format of a literature review because there is very little formal research on identity theft *per se*."
- "The biggest impediment to conducting scientific research on identity theft and interpreting its findings has been the difficulty in precisely defining it."
- "There is no national database recorded by any criminal justice agency concerning the number of identity theft cases reported to it, or those disposed of by arrest and subsequently prosecution."
- "Falseat present no way to determine the amount of identity theft confronted by the criminal justice system."
- "Most police departments lack any established mechanism to record identity theft related incidents as separate crimes."[44]

Further, in a Summer 2006 publication in the *Journal of Economic Crime Management* titled *The Ongoing Critical Threats Created by Identity Fraud: An Action Plan*[45] authors Gary R. Gordon and Norman A. Willox raise, among others, the following points:

---

41. U.S. General Accounting Office, Identity Fraud: Information on Prevalence, Cost and Internet Impact is Limited (1998), *available at* http://www.gao.gov/docdblite/info.php?rptno=GGD-98-100BR.

42. Graeme R. Newman & Megan M. McNally, Identity Theft Literature Review (2005), http://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf. The report was prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting to develop a research agenda to identify the most effective avenues of research that will impact on prevention, harm reduction and. *Id.*

43. *Id.* at 5.

44. *Id*. at iv-vi.

45. Gary R. Gordon & Norman A. Willox, Jr., *The Ongoing Threats Created by Identity Fraud: An Action Plan*, 4 J. Econ. Crime Mgmt. 1, 1 (Summer 2006).

- "While there has been significant attention focused on identity theft issues, little progress has been made to quantify the size and scope of the problem."
- "Little progress has been made in developing a national database of identity fraud incidents."[46]

And finally, the latest GAO report on IDT and data breach notification published in June 2007 indicated that little has changed regarding the lack of comprehensible, reliable data on ID theft. The title is perhaps the giveaway here: *Personal Information: Data Breaches Are Frequent but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown*.[47] Essentially, while there have been some minor improvements at the state level, industry, policy makers, and law enforcement are basically "flying blind" when it comes to an accurate measurement, and therefore lack understanding of the scope and nature of IDC in America.[48]

This lack of objective and reliable methods to measure IDC is one of the hallmarks of the broader issue concerning cybercrime and digital security. Simply put, there is insufficient accurate data on cybercrime (of which IDC is a subset) upon which to draw reliable conclusions and make influential economic and social decisions.[49] For the most part, the data available and most quoted is anecdotal and therefore of limited utility.

1. *A Cracked Definitional Foundation*

Pinpointing the definition of what constitutes ID theft is a prerequisite to determining liability for its occurrence, crafting incentives for preventing and responding to IDC, developing reliable measurements of its scope, and ascertaining whether or not society is in the midst of an IDC "crisis." We suggest that stakeholders are defining what ID theft is, and when it occurs, based on incomplete, or at times inaccurate or misleading information. The adequacy and question quality of the information was touched upon in the previous section.

---

46. *Id.* at 1-2.

47. U.S. GOVERNMENT ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007), *available at* http://www.gao.gov/new.items/d07737.pdf [hereinafter PERSONAL INFORMATION].

48. *Id.* at 4 (reporting that North Carolina and New York now maintain centralized databases on data breaches). This is a significant step in firming the reliability of digital crime data.

49. *See* Friedrich von Hayek, *The Use of Knowledge in Society*, 35 AM. ECON. REV. 519 (1945), *available at* http://www.virtualschool.edu/mon/Economics/HayekUseOfKnowledge.html (characterizing the economic problem as "a problem of the utilization of knowledge which is not given to anyone in its totality").

Until the defining of IDT evolves from a self-serving, discretionary exercise to one that anchors on existing statutory definitions or some other authoritative consensus, measurements and responses will continue to be divergent and/or contradictory. Implicit in any definition of IDT is the element of *when* the theft is deemed to have occurred, thereby carrying significant consequences for *where* to allocate the responsibility to prevent IDT as well as where to assign liability for any recoverable damages or losses due to IDT.

A major reason for the confusion surrounding IDT is the disagreement over its definition. That definition breaks down along two broad playing fields: criminal law and civil law. From a criminal law perspective there are investigatory and prosecutorial challenges when charging someone with IDT, which certainly affect IDT crime statistics.[50] However, the prosecution of identity theft is largely ministerial insofar as it is anchored around the plain language of a criminal statute. When an individual is criminally charged with IDT the courts will simply look to the relevant statute for the definition. The elements are laid out and then compared to a set of facts in the particular case. While there are two main types of criminal statutes defining ID theft, one that is triggered by the subsequent *use* of the data taken, and the other triggered by the *intent to use* the data in an unlawful manner, this paper suggests in the criminal context that this is a relatively straightforward decisional process. While there may be the usual strategizing and evidentiary challenges in proving the elements, there is little to no confusion that the plain language of the statute is the controlling authority for defining the crime of IDT.[51]

---

50. For instance, an identity thief may be charged with any number of criminal violations that may be a subset or superset of the specific IDT penal code section, not to mention that stats only reference the highest charge. In California, there are some 66 charges within the Penal Code that can be/have been related to IDT. Examples include: Forgery of Check; Possession of a Forged Instrument; Making, Possessing, and Uttering Fictitious Instruments; Acquisition of a Stolen Card; Sale or Receipt of an Access Card to Defraud; Acquiring Access Card; Acquiring Access Card Account Information without Permission; Changing Access Card so Other Than Cardholder is Billed; Pretending to be a Credit Card Holder without Consent; Petty Theft –Using Fictitious Access Card; Possession of Incomplete Access Card; False Personation; Use Personal Identifying Information of Another.

51. DEL. CODE ANN. tit. 6, § 12B-102 (2008) (effective June 28, 2005). For instance, Delaware's law reads: "if the investigation determines that the misuse of information about a Delaware resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Delaware resident." But California's Civil Code, section1798.29 reads: "(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." CAL. CIV. CODE §1798.29 (2008).

Understandably, the definitional problem has thus far been portrayed as a lack of uniformity between and among the definitions in the forty-nine state statutes and the two primary federal statutes.[52] But, is that currently the definitional malady that is obstructing one's ability to accurately assess the nature and scope of IDT? One novel contention is that the overlooked problem with defining IDT festers outside of the criminal arena. The key battle on the definitional front occurs on the civil turf, and more specifically, within the emerging world of data breach notification jurisprudence. For it is here where society is confronted with the reality of over seventy-nine million breached files[53] occurring as a result of data breaches. How institutions handle these breaches influences the citizens' and legislators' beliefs and perceptions about the prevalence of IDC in the U.S. The foremost shaping of those perceptions lay with society's system of jurisprudence, where the IDT is implicitly being defined in lawsuits within the context of perhaps the greatest threat to PII –data breaches.

What has emerged, therefore, are two pools of IDT data –traditional crime statistics from law enforcement reports and invalidated reports and claims seeking civil remedies for identity misappropriations. On the civil turf the parties involved are not attempting to collar the perpetrator for committing the crime of IDT against them, rather, they are seeking to hold PII holders responsible for harm to them that results from the unauthorized access of that PII.

The issue is not who is at fault, but who should bear responsibility, and specifically, when that responsibility is triggered. The significant nuance is that in seeking civil liability for IDT, parties are not referencing any of those plain statutory definitions to make the first order determination of when and if IDT occurs in order to support their claims that the data holders should be held responsible. This disregard of statutory definitions and reliance on an argument that ID theft has not occurred via "unauthorized access and transfer of personally identifying information by someone with the intent to use the data in an unlawful or wrongful manner," forces victims to remain virtually frozen in a reactionary posture.[54] Policy (whether via judicial rulings, legislation or regulation)

52. *See* NEWMAN, *supra* note 42.

53. This figure is the estimate provided by the San Diego-based Identity Theft Resource Center ('ITRC"). Mark Jewellap, *Record Number of Data Breaches in 2007*, Dec. 30, 2007, *available at* http://www.msnbc.msn.com/id/22420774/. Attrition.org, on the other hand, claims the figure is 162 million "records. *Id.* "Attrition.org and the Identity Theft Resource Center are the only groups, government included, maintaining databases on breaches and trends each year." *Id.* We employ the words "files" and "records" here to connote information held in a database containing personally-identifiable information directly relating to an individual.

54. NEWMAN, *supra* note 42.

that makes citizen-victims wait for their PII to be actually misused in order to claim the theft occurred and recover damages reinforces a legal regime that disincentivizes responsibility for preventing the harm from the loss of PII. So we cannot compare and accrue apples to apples across the civil and criminal IDT cases, but in addition to ongoing challenges and failures to resolve IDT criminally,[55] we have a poor inventory of the "apples" in the civil orchards that comprise the majority of the IDT harvest.

a. Statutory Definitions of ID Theft

The Identity Theft Assumption and Deterrence Act of 1998 ("ITADA"),[56] the first federal statute to define ID theft as a "stand alone" crime, defines it as:

> [to] knowingly transfer[ ], possess[ ], or use[ ], without lawful authority, a means of identification of another person with *the intent to commit*, or to aid or abet. . . any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law. . .[57]

We argue that the "intent" standard articulated in this statute must signal a concern on the part of the Congress with the simple access to and transfer of the data in question, as opposed to a requirement of misuse of the data. This language in the ITADA is proof that Congress was aware of the harmful and pernicious effects of this data simply being in the wrong hands, irrespective of the eventual use or non-use the data in question. If this posture is correct, the ITADA definition of when ID theft occurs calls into question numerous court decisions in negligence claims which found that losses sustained for heightened credit monitoring services and other claimed harms are not recoverable because they are incurred for fear of *future* injury from future ID theft.[58] Regardless of how the losses are characterized or how little time has passed since the breach, if the federal statute carries any authoritative guidance, and if the data can be shown to be the target of the breach, ID theft has already occurred and the individuals in question are victims of an ID theft.

---

55. *See* von Hayek, *supra* note 48. It is by no accident that IDT is well-accepted as a low risk, high reward crime.

56. Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318 § 5, 1998 (112 Stat.) 3010 (codified as 18 U.S.C. § 1001) [hereinafter ITADA].

57. 18 U.S.C. § 1028(a)(7) (2006) (emphasis added).

58. *See, e.g.,* Am. Fed'n of Gov't Employees v. Hawley, 543 F. Supp. 2d 44 (D.D.C. 2008). This includes but is not restricted to: emotional distress, legal fees incurred as a result of receiving notification of a data breach, future financial harm, damage to credit record. *Id.*

On the other hand, The Fair and Accurate Credit Transactions Act ("FACTA"), which amended the Fair Credit and Reporting Act ("FCRA"),[59] defined identity theft in a civil rather than criminal context noting that:

> The term "identity theft" means a fraud[60] committed using the identifying information of another person, subject to such further definition as the [Federal Trade Commission] may prescribe, by regulation.

It is logical to expect that in a negligence claim, given that it is a civil matter, the court and stakeholders will employ the FACTA definition. As mentioned, there are strong policy arguments that suggest the courts and stakeholders should do otherwise. The reason for noting this "definitional purgatory" is not to argue which statutory definition should govern, as policy is discussed later in the paper. The point here is to advocate that whatever definition governs in data breach cases, the rationales and decisional underpinnings should be explicitly and transparently present in the discussion of ID theft. It is the lack of transparency, and indeed, lack of any debate on the issue that this paper laments.[61] Long overdue, such a debate would have a profound impact on how data breaches are prevented and responded to since the definition is vital to the allocation of responsibility. Such a debate, when understood by the academics in question, will go a long way to substantiating and clarifying the ID theft literature that serves to raise public awareness and inform policy related to data breaches.

> The three manifestations of this cracked definitional foundation in the civil turf are:
>
> 1. Courts and attorneys in data breach negligence lawsuits that grapple with what will trigger recoverable damages/losses for the victims whose identities are compromised from the breach.
> 2. Organizations challenged to comply with statutorily-imposed duties to safeguard PII which has been compromised in a data breach.
> 3. Researchers and policy analysts in the private and public sectors who are tasked with profiling the extent and nature of ID theft across various demographics.

The current processes employed by all three stakeholders identified above are a cause and effect of the cracked definitional foundation in

---

59. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 2003 (117 Stat.) 1952 (codified as amended at 15 U.S.C. §§1681a-1681x) [hereinafter FACTA], *available at* http://www.ftc.gov/os/statutes/031224fcra.pdf.

60. We suggest it is worth keeping in mind that there are two traditional and contradictory legal definitions of the word "fraud." The more restrictive definition limits the term to financial wrong. The more expansive definition defines the term as, in general, something "wrongful" done to the victim. Employing the latter term could mean that the unlawful transfer of a person's PII is enough to trigger the FACTA definition.

61. The debate does threaten to break out in one case, *Pisciotta v. Old Nat'l Bancorp,* discussed *infra*.

that the parties involved employ specious decisions guided by opaque reasoning and often inconsistent or incomplete methodologies. This confluence creates responsibility shifting, misplaced liability determinations, and contradictory public policy decisions.

i. Courts and Attorneys

It is in both individuals' and society's interests that proactive steps are taken to prevent IDC. Responsibility can be allocated for proactive measures in a variety of ways, ranging from leaving individuals to bear the risk of the theft of their personally identifiable data, to spreading the risk across society. Currently, when an individual whose identity is compromised in a data breach receives notification, he is initially challenged to ascertain how likely he is at risk of further injury and contemplate taking reactive and proactive steps. Should he engage proactive steps such as credit freezing, if in fact he is eligible for such, or take reactive steps such as credit fraud monitoring to at least limit the potential for suffering harm?[62] When should these measures be undertaken?[63] Individuals may be reluctant or incapable of bearing the cost of measures necessary to diminish risks that are created by events out of their control and through no fault of their own. Or, they may simply be confused by how to respond and therefore hire professionals to provide guidance and services.

Traditionally in the current legal system, victims can recover for harms they incur under negligence or strict liability theories. However, the victim of a data breach is confronted with a conundrum that pits the strictures of the law against the realities of IDT victimization. The law demands a showing of actual injury as a result of the breach.[64] Is the

62. *See* Wikipedia, *Credit freeze*, http://en.wikipedia.org/wiki/Credit_freeze (explaining "[a] credit freeze, also known as a credit report freeze, a credit report lock down, a credit lock down, or a credit lock, allows an individual to control how a U.S. consumer reporting agency [also known as credit bureau: Equifax, Experian, TransUnion] is able to sell his or her data.") (as of Apr. 7, 2009, 22:40 GMT). The issue of eligibility to file a credit freeze stems from that fact that there are several legal hurdles one must navigate around before one can seek a credit freeze.

63. This information is based, among many other things, on the authors' combined experience with dozens of prospective clients who have consulted the authors in the wake of receiving a letter informing that their information may have been compromised as a result of a security incident. The language in the notification letters often resemble something like the language posted on a VA website. For example, "The Department of Veterans Affairs believes it is good practice for all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions, and to immediately report any suspicious or unusual activity." Latest Information on Veterans Affairs Data Security, http://www.usa.gov/veteransinfo.shtml# should (last visited Apr. 11, 2009).

64. *See* ANDREW SERWIN, PRIVACY 3.0 – THE PRINCIPLE OF PROPORTIONALITY, (West Publications 2008). The author states:

compromise of PII and the consequent need for preventive measures injury, in and of itself, or is that only speculative injury from potential future misuse of the data? Does ID theft, the tortious injury, occur when the data was taken or only if the data is subsequently misused?

This is a crucial distinction for victims of IDC and officers of the court who serve them, for the answer has significant consequence for individuals' recoveries, preventive safeguards for future victims, and public policies about how IDC losses are amortized. If IDC injury (actual injury) occurs when the data is taken, the costs should be borne by the party who could more efficiently[65] prevent the harm from the breach.[66] If on the other hand, the ID theft injury is deemed not to have occurred until some speculative time in the future when the data is misused in a manner that can be specifically traced back to the breach, then it is less clear who should bear the cost of prevention.

Surprisingly, inasmuch as the published opinions shed any light on the matter, victims' attorneys in data breach class action lawsuits have disregarded the statutory definition guidance and have instead framed the issue as a matter of prevention of future injury from ID theft.[67] In the immediate wake of a data breach which exposes victims PII, and in the absence of ID theft statutes which define it otherwise, it may seem commonsensical for attorneys to craft their case around the presupposition that ID theft has not yet occurred.[68] However, in the face of existing statutory definitions that assert otherwise, and if relied upon would eliminate the need to persuade the court to embrace innovative damages

---

> Both Warren and Brandeis, as well as Prosser, explicitly rely upon tort enforcement for privacy violations. However, a model that relies upon tort enforcement is doomed to inconsistent results because relying upon tort enforcement ignores the reality that many privacy breaches that should give rise to a remedy of some sort, particularly in the case of truly sensitive information, do not because there is no "damage" suffered by the individual as a result of the breach. As discussed below, this has been an issue for courts, and will continue to be one as long as we rely upon common law models.

Id.

65. By "efficiently" we mean the best result for the lowest cost.

66. Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181, 184 (1996) ("Where multiple parties [i.e, either customers or financial institutions] could take . . . precautions, regulations, should, therefore, place the obligation in the party who can avoid the loss at the lowest cost.") (citing Robert D. Cooter & Edward L. Rubin, *A Theory of Loss Allocation for Consumer Payments*, 66 TEX. L. REV. 63 (1987)).

67. In all of the cases we have reviewed, it appears to us that the plaintiffs' attorneys have operated pursuant to a theory that the unauthorized acquisition of compromised data is not, in itself, ID theft.

68. Having not accessed the briefs that would shed light on this decision we are only left to infer that the attorneys reached this decision given that the judges in question assume the matter has been put to rest. Had this not been so, one would expect to see more of an argument from the judge regarding why the attorneys had reached the wrong conclusions regarding what is ID theft and when had it occurred.

theory, commonsense be damned. As revealed below in an examination of cases where the defining of ID theft was seminal, the plaintiffs would have been better served by availing themselves of an existing definition and not the one they ultimately advocated.

Unsurprisingly, courts have accepted victims' counsel's presentation of the issue and have thus concluded that since actual injury has yet to occur, the costs incurred to prevent future harm are not recoverable.[69] The result is usually case dismissal on the grounds that the requirement to show harm, a necessary element in any tort case, has not been met.

The reasons for the judiciary's passive acceptance of this definitional framing are hard to ascertain. To be sure, it is not the judge's role to raise the issues and make the case given victims' counsel's failure to present the IDT as a current injury under a statutory reading of the definition of IDT. However, it is certainly not unheard of for courts to use discretion and take an active role in issues where public policy considerations demand that determinations of responsibility be embraced. We advocate that the public policy issues raised by IDT justify such engagement.

It is now necessary to shift from officers of the court to organizations incurring a data breach to further illustrate where individuals are making decisions predicated on unfounded assumptions about the definition of ID theft.

ii. Entities That Have Experienced a Data Breach

In the wake of detecting a data breach the organizations often have a legally imposed duty, via data breach notification ("DBN") statutes, to determine whether they must disclose the breach to the individuals who's PII has been compromised.[70] This has the practical effect of alerting the general public of the breach.

Initially, this determination did not allow for much discretion.[71] If the data was unencrypted and breached, the notification requirements were triggered. However, as numerous states followed California's lead

69. We say "unsurprisingly" because our legal system is predicated on an adversarial basis which means the court leaves it to the two party adversaries, the plaintiff and the defendant, through their lawyers to raise and frame issues. If one side wants to 'give away' a point that may not be in their ultimate interest, the court, to the extent it can spot the give away in the first place, will clearly oblige the party in question.

70. For a listing of state data breach notification laws, *see* State Breach and Freeze Laws, http://www.pirg.org/consumer/credit/statelaws.htm#breach (last visited Apr. 11, 2009).

71. For example, California's data breach notification law applies a strict standard for notification. Aside from exceptions for good faith acquisition, encrypted data, and delay to facilitate investigation by law enforcement, the law requires notification after unauthorized acquisition of PII. S. B. No. 1386, 2002 Cal Adv. Leg. Serv. 915 (Deering) (codified as amended in CAL. CIVIL CODE §§ 1798.29, 1798.82 (Deering 2002)).

in passing DBN statutes, the statutory duty to notify became more intricate, allowing for considered judgment by breached organizations.[72] Some states began to require a self-determined finding that the individuals were at risk of some future harm, sometimes explicitly from ID theft, before the duty to notify was triggered.[73] Proposed federal law which includes a provision to preempt all state DBN laws would require this determination of the risk of future harm from ID theft be made before triggering the notification duty.[74]

Such statutes implicitly obligate the breached entities to define ID theft in order to assess whether there is risk that it has or will occur as a direct result of breach.[75] Note that no criminal charges for ID theft against a breached company are triggered as a result of the breach, and therefore no specific statute governs the definitional assessment upon which the notification is based.[76] In essence then, the breached organization is free to use its own standards in reaching a decision. This is clearly a decision fraught with conflict of interest. On one hand, if it concludes that the trigger has been met (that there is a risk of harm to the individuals in question) the entity exposes itself to significant expenses. These may include, at minimum, negative publicity and loss of public confidence, notification costs and customer attrition.[77] If the company is publicly traded, additional costs may involve stock devaluation

72. FACTA, *supra* note 59.

73. *See, e.g.,* CONN. GEN. STAT. § 36a-701b (2008) (effective Jan. 1, 2006) (applying a likelihood of harm standard); WASH. REV. CODE § 19.255.010 (LexisNexis 2008) (effective July 24, 2005) (using a standard of reasonable likelihood of risk of criminal activity); DEL. CODE ANN. tit. 6, § 12B-102 (2008) (effective June 28, 2005) (using a likelihood of misuse standard).

74. *See* United States Senator Dianne Feinstein, California, Protecting Your Identity, http://feinstein.senate.gov/public/index.cfm?FuseAction*sueStatements.View&Issue_id=5b8dc16b-7e9c-9af9-7de7-22b24a491232 (last visited Aug. 29, 2008).*

75. *Supra* note 70. The various state data breach notification statutes are distinct from the respective state identity theft statutes. Nevertheless, the trigger for notification involves assessing whether the threshold has been met. This threshold is quite often based upon the existence or likelihood of identity theft. Therefore, covered entities anchor notification triggers around the definition of identity theft. For example, Arizona's notification requirement is triggered where the breach of security "causes or is reasonably likely to cause substantial economic loss to an individual."). *Id.*

76. There may be criminal actions triggered concerning the unauthorized access and taking of data, but no first party criminal IDT liability for the breached company.

77. PONEMON INSTITUTE, LLC, 2007 ANNUAL STUDY: U.S. COST OF A DATA BREACH 2 (2007). More specifically, costs may include: consulting costs for investigation, attorney's fees, and crisis management; notification letters send via certified mail; establishing a call center, including incident media expense for the notification/crisis management; credit monitoring costs; and, fines, fees, compliance expenses and defense costs related to regulatory investigation and compliance. *Id.* Research by the Ponemon Institute estimates that in 2007 the average cost of a data breach was $197 per record, with an average total cost per company of more that $6.3 million. *Id.*

related to potential legal proceedings, Securities and Exchange Commission quarterly reporting and general shareholder concerns related to the aforementioned data breach expenses.[78]

On the other hand, if the breached entity concludes that there is little or no current or future risk of ID theft as a direct result of the breach, the entity can lawfully bury knowledge of the breach and the persons whose identities have been exposed are none the wiser.In such cases, there is no public awareness that the event occurred, let alone how the risk decision was made. In lieu of knowledge about how these first order definitional decisions lead to statutory compliance, it can be surmised that organizations utilize some "methodology" to guide their risk analysis of the likelihood of ID theft in the wake of a data breach. Academic and policy research literature on ID theft is a reasonable bet, yet as described below, it is the third arena that perpetuates and reflects unarticulated assumptions about the definition of ID theft.

iii. Researchers and Analysts

The vast majority of academic literature on IDT accurately recounts what IDT is and when it occurs in relation to the panoply of state and federal statutes.[79] In so doing, while they are correct in attributing the inconsistency in definitions across statutes as a hurdle to understanding the scope of the problem, they also neglect to account for the non-state statutory charged instances of IDT in civil data breach cases. Similar to the judicial approach, it must be inferred that their definition of IDT is based on a use-manifestation of damages genre of the IDT definition. This is to be expected because academic and policy research literature anchor off of state identity theft criminal laws and statistical reporting related to same. Therefore, researchers' and analysts' portrayals of the definitional issues focus narrowly on squaring the labeling inconsistencies that arose when the crime of identity theft was afforded its own charge in the midst of legacy law enforcement practices that dealt with IDT under a host of existing crimes involving the use or abuse of financial instruments and/or another's identity.

For example, IDT was often charged across a spectrum of crimes, including check fraud, forgery, theft (robbery, burglary) and other species of fraud.[80] In focusing on this one slice of the pie comprising IDT,

78. If there is a likelihood of a "material loss" to the company, based on the company's total capitalization and annual revenues, that company must report it Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. 15 U.S.C. § 78m (2006); 15 U.S.C. § 78o (2006). While we do not claim that there automatically will be reason to assume a company will suffer a likelihood of a "material loss" as a result of a data breach, we do think it possible and, in some cases, probable.

79. *See* Gordon & Willox, *supra* note 45, at 1; NEWMAN, *supra* note 42.

80. Newman characterized the definitional problem as follows:

existing research literature fails to acknowledge the intent-to-misuse definition,[81] which is grounded in law other than state penal codes. This presupposition of the definition of IDT overlooks vast numbers of cases, such as those noted above in data breach situations, and paints a picture of the scope and prevalence of its occurrence that has quite a different affect on decisions concerning liability, responsibility and public policy regarding IDT.

For example, ID Analytics' oft-quoted white paper on ID theft is referenced in the wake of a data breach.[82] It purports to put a probability on the number of ID thefts that occur in the wake of a breach, but never does it specify or account for the definition of ID theft upon which these probabilistic conclusions are calculated.[83] Decision makers and the citizenry at large are blissfully unaware of who makes these definitional decisions, what the criteria are for the decisions, and what the rationale is for flouting the intent-based definition espoused in authoritative statutes. The consequence is that opaque conclusions are rendered on issues that are of profound importance to society. What is more disconcerting is that individuals, institutional stakeholders, policymakers and courts likely rely on these academic and pseudo-academic conclusions as a basis for their perceptions, beliefs and actions in addressing IDT in their respective capacities. Discussion now turns from addressing the definitional issues in an abstract manner to demonstrating how they play out in more concrete negligence cases resulting from several notorious data breaches.

b. The Department of Veterans Affairs Data Breach of 2006

In June 2006, close to twenty-five million military veterans' data

---

> The biggest impediment to conducting scientific research on identity theft and interpreting its findings has been the difficulty in precisely defining it. This is because a considerable number of different crimes may often include the use or abuse of another's identity or identity related factors. Such crimes may include check fraud, plastic card fraud (credit cards, check cards, debit cards, phone cards etc.), immigration fraud, counterfeiting, forgery, terrorism using false or stolen identities, theft of various kinds (pick pocketing, robbery, burglary or mugging to obtain the victim's personal information), postal fraud, and many others.

NEWMAN, *supra* note 42, at 5.

81. As discussed, the ITADA defines ID theft has having occurred at the time of the unauthorized access and transfer of identifying data, if accompanied with an *intent by the individual who took the data* to misuse it in some unlawful manner. *See* ITADA, *supra* note 56.

82. *See* Press Release, ID Analytics, Inc., Data Breach Harm Analysis from ID Analytics Uncovers New Patterns of Misuse Arising from Breaches of Identity Data (Nov. 7, 2007), *available at* http://www.idanalytics.com/news_and_events/20071107.html; Carl Weinschenk, *Study of Stolen Identity Use Patterns Offers Surprises*, ITBusinessEdge, Aug. 13, 2008, http://www.itbusinessedge.com/item/?ci=46755.

83. ID Analytics, *supra* note 82.

was accessed and transferred in an unlawful manner.[84] The breach occurred as a result of a daytime break-in at the home of a VA employee who had the data stored on an external hard drive apart from its accompanying computer housing.[85]

Did the veterans in question suffer ID theft as a result of the breach? There is a strong case supporting an affirmative answer given that identifying information about the Veterans was 'transferred"—(removed from the employee's possession and control in his home, by someone who lacked "lawful authority") by a home intruder, with the "intent" to use the data to perpetuate future unlawful activity. This is especially true in light of the unlikelihood that the break in and absconding with the hard drive could be tied to a legitimate purpose.

Critics may challenge the intent element by arguing that the burglars may have only been targeting the computer hardware and not the data contained therein. A host of facts from both first source and media reports, however, support the intent element.[86] Specifically, the hard drive containing the data was twice removed from the computer encasing –it was located in a bedroom nightstand, separated from the body of the computer which was located in another room on an entirely different floor in the home.[87] Further, the external drive was primarily composed of a vast treasure trove of PII, and there were few items stolen during the burglary, if any at all. At a minimum, a rebuttable presumption has been established that the intruders broke in to obtain the data in the hard-drive because it could be used to provide them benefit. Since the legitimate uses of that stolen PII are hard to imagine, the intended unlawfulness of its use is an easy sell. Under this line of reasoning, the veterans whose data was compromised are indeed the victims of ID theft (injury) as a result of the negligence of the VA and the employee in question, and therefore are entitled to reimbursement for any costs they may have incurred attempting to prevent future harm from this ID theft (injury).

It is important to reiterate that the federal statute on ID theft is not controlling here. That is, there are no individuals in the VA case charged with the crime of ID theft. If that were the case, the statutory definition would certainly be controlling. Nevertheless, in cases where the relevant, controlling statute(s) do not offer precise definitional guidance (such as the case with negligence claims for identity theft) it is reasonable to turn to the federal statute as an authoritative guide in determin-

84. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Aug. 17, 2008).

85. *Id.*

86. Ken McClain, General Counsel for the U.S. Department of Veterans Affairs, Address at the IAPP Privacy Academy (Oct. 26-28, 2005).

87. *Id.*

ing whether ID theft (injury) has occurred.[88]

The standards for defining when ID theft occurs can be characterized as detection versus manifestation, with the former based on "intent to use unlawfully" and the latter predicated on "provable unlawful use." The detection standard is triggered by the existence of *notice*on the part of the relevant entities and individuals in question that the data has been taken in an unauthorized manner with the intent to use it in the future for an unlawful activity.[89] The manifestation standard, on the other hand, is triggered only by subsequent notice and confirmation that the data in question has been used in some wrongful manner, usually resulting in harm to the victim, and that such use has a legally sufficient causal relationship to the initial theft of the data in question.[90]

The detection standard is a preemptive standard, in that it permits and calls for action to *prevent or at least limit* any subsequent harm and places the burden for preventing the harm on the shoulders of the party responsible for the harm in the first place. This is the party whose negligence was found to be a contributory cause for the breach. The manifestation standard, on the other hand, is a reactive standard in that it requires the victims to wait until the harm explicitly manifests itself, and can be proven to have been directly related to the theft in question. This puts the onus for preventing any *further* harm on the victim, since some harm from the misuse of the data has to occur first before liability is triggered. This is standard upon which the vast majority of courts have settled.

This examination of the VA data breach exemplifies the consequential significance of the unstated definitional battle in the immediate aftermath of a data breach. This paper now turns to a case that contained

88. We acknowledge that in the VA case the issue of losses incurred for heightened credit monitoring would be moot here given that the VA offered to pay for any such costs. Notably this was in exchange for the compromised individuals agreeing to give up all other civil claims they may have had.

89. Ken McClain, General Counsel for the U.S. Department of Veterans Affairs, Address at the IAPP Privacy Academy (Oct. 26-28, 2005. 'Notice" in legal terms can be actual or constructive. BLACK'S LAW DICTIONARY 484 (2d Pocket ed. 2001). Actual notice is "notice given directly to, or received personally by, a party." *Id.* Constructive notice is notice that arises without regard to actual notice, but as a "presumption of law from the existence of facts and circumstances that a party had a duty to take notice of. *Id.*

90. *See, e.g.,* RESTATEMENT (SECOND) OF TORTS § 281 cmt. (1965). Legal causation is a two-part analysis. *Id.* The first question is whether there is a factual link between the defendant's act [or failure to act], and the plaintiff's harm. *Id.* The second question is more of a policy question, and concerns whether it is in the interests of public policy to hold the defendant liable under the circumstances. *Id.* If the link between the cause and the harm is too attenuated, or the chain of causation is broken by an intervening event, the defendant will generally be found not liable. *Id.*

many of the same elements of the definitional battle in the wake of negligence claim emanating from a data breach.

c. Tracy L. KEY v. DSW, Inc.[91]

The fact pattern is familiar enough. The court noted that:

> Between November 2004 and March 2005, Defendant, DSW, collected and maintained credit card, debit card, and checking account numbers and other confidential personal financial information of approximately 1.5 million consumers who purchased merchandise at DSW retail outlets. . . . Because of DSW's alleged improper retention and failure to secure this information, on or about March 2005 unauthorized persons obtained access to and acquired the information of approximately 96,000 customers.[92]

Tracy L. Key ("Key"), the lead plaintiff in the class action suit, claimed that as a result of the breach she, and the rest of the class:

> . . .have been subjected to 'a substantially increased risk of identity theft, and have incurred the cost and inconvenience of, among other things, canceling [sic]credit cards, closing checking accounts, ordering new checks, obtaining credit reports and purchasing identity and/or credit monitoring.[93]

This excerpt, taken from the plaintiffs' complaint, thus implies its lawyers decided that ID theft had not occurred in this case. The court and, one would conclude, the defendant's attorneys, were only too ready to work within the cracked definitional framework the plaintiffs' lawyers provided it. No reasons are proffered for this rather startling stipulation on the plaintiffs' part. The judge, as a result, felt free to address the relevant damages as issues of fear of future harm, as manifest by his use of the word "future" twenty-one times throughout the five-page opinion.[94]

Specifically, citing *Forbes v. Wells Fargo*,[95] a somewhat[96] similar data breach case, the court noted that the plaintiffs in *Forbes*, like the plaintiffs in *Key*, contended that the time and money they spent monitoring their credit sufficed to establish damages.[97] The Forbes court rejected that contention and granted summary judgment to the defendant

91. Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006).

92. *Id.* at 687.

93. *Id*. at 688-89.

94. *Id.*

95. Forbes v. Wells Fargo Bank, 420 F. Supp. 2d 1018 (D. Minn. 2006).

96. This case was only "somewhat" similar. We would argue there is a substantial difference between stealing hardware, where the target may be the hardware and/or the data on the hardware versus a remote intruder who hacks in to a computer or network looking only for the data on the system. In the latter case we assume there is indication of intent to use the data in some wrongful manner.

97. *Forbes*, 420 F. Supp. 2d at 1020.

on all counts.[98] Like the *Forbes* court, the court in *Key* emphasized that the plaintiffs had overlooked that their injuries were solely the result of a "*perceived risk of future harm*."[99] The court stated that the "[plaintiffs] overlook the fact that their expenditure in time and money was not the result of any *present injury, but rather the anticipation of future injury* that has not materialized."[100] Consequently, the court ruled that the "plaintiffs failed to establish the essential elements of damages."[101]

How is the court defining injury from ID theft then? Certainly not by reference to the ID theft Deterrence Act as the term "injury" is commonly understood. The court went on to expound at length why this case was best understood under the *Forbes* definition of harm and injury absent any discussion of why it deemed the *Forbes* rationale valid and applicable to *Key*.[102] Such opaque discussion of important public policy does not serve society well since it perpetuates poorly articulated, definitional assumptions. This ruling, and its like, which adhere to the "manifestation" standard discussed subsequently, will do little to reduce the "future harm" the citizens may suffer from a chaotic digital environment. Indeed, it may very well exacerbate the risk of harm in a digital environment, where because of the tight coupling of actions and cascading damages, the cost of preempting damage will be less than trying to identify and remediate harms afterwards.

2. *Quantifying the Problem –Groundhog Day*

Another consequence of the definitional quandary is the lack of empirical data about the incidence of IDT. As noted in the preceding section, experts have pointed out the difficulties in quantifying IDC, and specifically, IDT, are compounded by the lack of a precise definition of the crime, and/or act, itself.[103] The vast majority of "statistics" on IDC and IDT is information gleaned from what are often times self-serving surveys or self-reporting questionnaires.[104] To a great extent society is "flying blind" with regard to cybercrime and ID Theft.[105]

This method of collecting data on cybercrime is a dramatic shift away from the more traditional, brick-and-mortar crime problems. Examining the latter, society has a plethora of academic, scientifically based, first source literature. This acute lack of knowledge regarding

98. *Id.*
99. Key, 454 F. Supp. 2d at 690.
100. *Id.*
101. *Id.* (emphasis added).
102. *Id.*
103. Gordon & Willox, *supra* note 46.
104. *Id.*
105. This is by no means to imply that we are bereft of "information." Rather, we have a bounty of white papers and "peer review lite" article based on feeble underlying data.

cybercrime metrics is not new.[106] It initially manifested itself in 1982 at the first Congressional hearings that lead to passing the first comprehensive federal statue addressing cybercrime, the Computer Fraud and Abuse Act ("CFAA").[107] A brief examination of this history is called for.

At those hearings a 1982 Department of Justice Report, entitled "Electronic Fund Transfer Systems and Crime," was cited as saying that "no valid data for measuring and understanding the nature and extent of EFT crime [electronic funds transfers]" existed.[108] At these same hearings the Department of Health and Human Services published a 1983 Report which concluded with the following: "[a]lthough originally charged to discover the scope of computer fraud and abuse in government programs the task force rapidly became aware this was not possible" due to lack of credible statistics.[109] This did not stop the passage of the law.[110] Furthermore, at those hearings, suggestions of a mandatory reporting system for cybercrime were discussed but ultimately rejected.[111] Now, twenty-five years later, little has changed with this issue in the context of cybercrime reporting. We are still debating the need for more reliable cybercrime statistics and better reporting regimes.

That very little has changed with regard to the concerns articulated at the 1982 hearings contributes to the haphazard reaction to the perceived ID theft crisis today. While there were justifiable excuses for lack of reliable data a quarter of a century ago, the same cannot be said for today. The alleged ID theft crisis is a specific example of how this lack of knowledge affects us today. Next to the definitional quandary, the related lack of reliable statistics is the second contributor to the crippled ability to know the nature and scope of IDT.

a. ID Theft Statistics –Battle of the Numbers

No matter how one tries to square it, citizen-victims are caught between multiple stakeholders: one group, law enforcement, does not want to be stuck with collecting and studying the data. A second group, business, is hesitant to provide the data in the first place. The third group is

106. Encarta English Dictionary, *metric*, http://encarta.msn.com/dictionary_/metric.html (defining "metric" as:"a standard or a statistic for measuring or quantifying something else").

107. 18 U.S.C § 1030 (2008).

108. *See* Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to Growing Problem*, 43 VAND. L. REV. 453, 459 n.41 (1990).

109. *Id.* at 460 n.43.

110. We are not arguing that it should have, but it *should* have sent a flare up as to what one of the major problems was in cybercrime, at a time when the United States was poised to move into cyberspace in a meaningful, widespread, and robust manner. Very little has been done to rectify this issue.

111. Griffith*, supra* note 108, at 460 n.43.

well-intentioned government and consumer advocate organizations tasked with marshalling citizen victims' concerns. Lastly, we have the commercial vendors who are quick to exploit the knowledge gap and information inefficiencies as they trumpet their "must have" products and services to address IDC. All of these stakeholders have vested interests in capturing and portraying IDT statistics.

This section begins with the third group by turning to the Consumer Sentinel, the Federal Trade Commission's national database for collecting ID Theft complaints from citizen-victims. Its creation was mandated by section 5 of the Identity Theft and Assumption Deterrence Act of 1998 ("ITADA").[112] It acts as the central repository for consumers to report incidences of "online" consumer fraud as well as ID theft. The FTC's first, and thus far only, comprehensive, multi-year survey on ID theft is an example of the reliability issues in cybercrime reporting.[113] The 2003 survey report estimated that twenty-seven million people had been victims of ID theft in the previous five years.[114] Coupled with the FTC-estimated 9.9 million (4.6percent of the population) between 2002 and2003 alone, the grand total was 38.9 million victims.[115] That is a smidgen short of one in four adults in the public at that time. By just about any standard of measure, one could safely argue this is a breath-taking figure.

Surveys debunking or at least claiming to debunk the FTC 2003 numbers were not long in coming.[116] Javelin Research[117] proffered that "in addition to the FTC's claim of 9 million victims of identity theft in 2004, the vast majority of complaints dealt with traditional forms of theft such as stealing wallets or checkbooks, as opposed to Internet-based fraud" and therefore FTC numbers were misleading.[118] In 2004 the FTC

112. ITADA, *supra* note 54.

113. FEDERAL TRADE COMMISSION., IDENTITY THEFT SURVEY REPORT (2003), *available at* http://www.ftc.gov/opa/2003/09/idtheft.shtm.

114. *Id.*

115. This estimate was based on a combination of phone surveys and complaints from Sentinel. *Id.* Operating under the assumption that x amount of people who are victims of ID theft never reported their theft to the FTC and comparing the non-reporting number with the total number of people who did respond, the FTC came up with the final figure of 38.9 million. *Id.*

116. Gartner's 2003 Survey had it at seven Million. *See* Press Release, Gartner, Inc., Gartner Says Identity Theft is up Nearly 80 Percent: 7 Million U.S. Adults Were Identity Theft Victims in the Past 12 Months (July 21, 2003), *available at* http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp.

117. For more on the Javelin Report cited, *see* Privacy Rights Clearinghouse, Identity Theft Surveys and Studies: How Many Identity Theft Victims Are There? What Is the Impact on Victims?, http://www.privacyrights.org/ar/idtheftsurveys.htm (last visited Oct. 17, 2008).

118. "Most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the method was known, 68.2% of information was

reported that there were nine million victims of ID theft fraud. This was down approximately one million from the final 2003 figure of 9.9 million.[119] However, a Department of Justice Survey the same year came in at 3.6 million.[120] The 2003 study is cited because it was billed as the most comprehensive study of ID theft done by the FTC, the agency mandated by Congress to collect statistics on ID theft. However, there are certainly more recent findings, though they fail to bring clarity to the issues of quantifying ID theft.

Market research firms Javelin and Gartner released studies in 2007 featuring contradictory claims that identity theft is both on the rise and decline.[121] The Gartner study claimed that ID theft in America had increased by "more than 50 percent since 2003."[122] On the other hand Javelin Strategy and Research cited that "fraud using personal data" was on a gradual [eight percent] decline from 2003.[123] The fact that two of the most cited statistical reports can reach such nearly opposite findings speaks volumes about the disparity and disagreement over IDT numbers. In the midst of this battle of statistics, the Federal Trade Commission reported that identity theft continues to be the top complaint received by the agency.[124] In 2006, thirty-six percent of complaints received by the agency were about identity theft.[125]

---

obtained off-line versus only 11.6% obtained online." *Id.* The authors contend that this premise, offered as an example of meaninglessness of many figures being bandied about, is utterly useless. Given that agonizing few database breaches were acknowledged prior to the passage of SB 1386 in 2003, the announcements have been nearly nonstop since then. How do we accurately ascertain where, over say, the last ten years thieves have gotten their booty?

119. *See* Consumer Sentinel, National and State Trends in Fraud& Identity Theft January - December 2004 4, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/clearinghouse_2004.pdf.

120. *See* Press Release, U.S. Department of Justice, 3.6 Million U.S. Households Learned They Were Identity Theft Victims During a Six-Month Period in 2004 (Apr. 2, 2006), *available at* http://www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm.

121. Javelin Strategy and Research, U.S. Identity Theft Losses Fall, http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/ (last visited Aug. 17, 2008); Press Release, Gartner, Inc., *Gartner Says Number of Identity Theft Victims Has Increased More than 50 Percent Since 2003* (Mar. 6, 2007), *available at* http://www.gartner.com/it/page.jsp?id=501912.

122. Press Release, Gartner, Inc., *Gartner Says Number of Identity Theft Victims Has Increased More than 50 Percent Since 2003* (Mar. 6, 2007), *available at* http://www.gartner.com/it/page.jsp?id=501912.

123. MSNBC.com, Study: 9.3 Million ID Theft Victims Last Year, http://www.msnbc.msn.com/id/6866768/ (last visited Oct. 14, 2008).

124. Press Release, Federal Trade Commission, FTC Releases Top 10 Consumer Fraud Complaint Categories (Jan. 25, 2006), *available at* http://www.ftc.gov/opa/2006/01/topten.shtm.

125. *Id.*

b. ID Theft Risk Analyses –A Data Sausage Factory?

It is reasonable to expect that a lack of data (the previously described porous foundation of ill-fitting and inconsistent definitions and suspect statistics) has engendered dubious analytical conclusions. Strained metaphors aside, the sausage is only as nutritious as the parts fed into the grinder.[126] This section argues that the defects associated with second order analyses (attribution, victimization and damages) are illustrative of a chaotic information framework perpetuated by the predominance of free market policy.[127]

Free market policy, which is contemplated as an acute deficiency in governmental regulation mandating the collection and reporting of IDC data, has both exploited and facilitated the knowledge gap between actual occurrences of IDT and recording of same. The values driving the current free market policy are not always advanced by promoting reliable analyses. Reliable analysis is not free. Reliable analysis is the product of cascading costs that come from knowledge- management and accountability costs, and liability and compliance costs, all of which evoke risk controls that can certainly be viewed as barriers to the free flow of information goods and business models.

For these nonexclusive reasons the market does not necessarily incentivize determination of causes and effects of past, current and future harms from IDC. Information, especially PII, is both a commodity and currency in our economy. Until the costs of unreliable information (via dubious attribution, damages and victimization analyses) grow beyond the benefits of the free flow of data, the market will not close that IDC knowledge gap. Sections 2 (B) and (C) described the ill-fitting puzzle pieces of statistics on the size and scope of IDC. The squabbling over second order analyses based on these statistics both further perpetuates, and is fueled by a chaotic information environment.[128]

---

126. This also presupposes that the "grinder" is "clean," i.e., there is no self-serving agenda operating on the empirical facts and data.

127. *See* Asher Shkedi, *Second-order Theoretical Analysis: A Method for Constructing Theoretical Explanations*, 17 INT'L J. QUALITATIVE STUD. EDUC. 627 (2004). As used herein, second-order analyses are those that interpret qualitative data gathered mainly from first-order accounts: the direct descriptions and explanations of IDT informants (victims, perpetrators, investigators, or other parties who participated in the IDC event). Second-order analyses, such as attribution, damages and victimization, are used in the absence of a full description and explanation of the IDC event and thus involve varying levels of inference on the part of the party producing the analysis.

128. For example, according to Chris Hoofnagle, an expert in data security, and an attorney at Berkeley's Center for Law and Technology:

> The FTC's Opinion on Javelin rejects Javelin's findings as 'misleading:' In an email to Wall Street Journal reporter Robin Sidel, obtained under the Freedom of Information Act concerning the Javelin Report, an FTC employee wrote: "Since most surveyed–74 percent–could not identify the person who stole their identity,

The market not only facilitates the knowledge gap, but exploits it as well. Specifically, the gap allows and encourages society to over-generalize about the relative risks present or absent in the digital environment. This overgeneralization, in turn, fuels the human desire to seek control and determinism in the face of chaos or danger. This is to say, it is a truism across all of human activity that in the face of information chaos, where determinism is severely deficient, humans seek to achieve a feeling of control, whether real or perceived. So, individuals and institutions oftentimes create social fictions to fulfill that need to cope and perceive themselves as secure. Coping mechanisms, to be sure, are not inherently bad. They are undesirable, however, to the extent that these social fictions are predicated on selective, incomplete and/or unverified data and are weaved to paint a "truth" that promotes one party's fortune to the detriment of many others. The following types of IDC analyses are illustrations of social fictions insofar as they claim to bring determinism to the IDC knowledge gap –attribution, damages, and victimization. To the extent that any of these analyses are based on impartial data and/or are intentionally manipulative in their motivations, they perpetuate and embed false and ultimately counter-productive perceptions.

i. Attribution Problem

One consequence of the data chaos is an obfuscation of the causes of illegal acquisitions and uses of identity artifacts, a dynamic which allows blame to be shifted to the entities with a weak collective voice. In this situation, it is the citizen victims. Stated differently, this lack of aggregate, first-order IDC data disincentivizes the private sector from taking rightful ownership of the problem. To be sure, ultimate responsibility for IDC resides with the criminal actor(s) and undoubtedly there is a heightened threat from the criminal element, including state-sponsored and

---

> and half the 26 percent who could identify the thief either didn't personally know the thief or said it was someone other than a friend or relative, it would be misleading to suggest that the 'Culprit is likely a friend or relative.'"

Comments of Chris Hoofnagle, *reprinted in* Ryan Singel, *Identity Theft Not Down, It's Different, Expert Says,* WIRED BLOG NETWORK: THREAT LEVEL, Feb. 2, 2007, *available at* http://blog.wired.com/27bstroke6/2007/02/identity_theft.html. *See* Martin H. Bosworth, *FTC Findings Undercut Industry Claims that Identity Theft is Declining*, Feb. 9, 2007, http://www.consumeraffairs.com/news04/2007/02/ftc_top10_folo.html. The article states:

> The FTC complaint findings serve as a counterpoint to industry claims that identity theft is somehow less of a threat these days. A study recently released by Javelin Research claimed that identity theft instances declined by 11.5 percent between 2005 and 2006, with 2006 losses declining to $49.5 billion.The Javelin study was funded by Visa, Wells Fargo, and check-printing company CheckFree.

Id.

enterprise crime.[129] However, because of technical, investigative and legal difficulties identifying, tracing, prosecuting and obtaining restitution from perpetrators, losses are shifted and spread among second-order "causes" of IDC. Attribution claims and associated recommendations abound. While there is clear disagreement about the causes of IDC (the illegal acquisition and uses of identity artifacts) there is consensus that all the vested interests have an opinion.

Ambiguity in identifying the source of data insecurity or responsibility for data stewardship facilitates the justification of any stakeholder's position when identities are compromised. As long as this IDC data inefficiency is allowed to flourish, social fictions and false perceptions will hold sway. Companies such as information brokers, merchants, financial institutions, and the credit reporting bureaus taking advantage of these fictions and perceptions will be allowed to absorb and shift losses associated with IDC. This will be done absent accountability for the wrongful party or transparent debate about who should bear the costs and who should implement the safeguards. Responsibility for the inevitable leak in the dyke and its necessary patches will never be accurately or efficiently addressed.

This is made difficult since computer security incidents in a networked environment often have cascading and multiplier effects.So breaches and attribution for resulting IDC does not break down linearly or cleanly between the purported "causes," or potentially responsible entities. As a result, responsibility and liability is a shared obligation when it comes to security in an interconnected society. Given this context, a reasonable accountability scheme should focus on entities at the upper end of the benefit-control continuum, where there is balanced proportionality between the benefits gained from having identity data and the ability to control the security and integrity of that data. While this proposition is not sparking rampant debate, this is less a reflection of agreement than it is the fact that there is scant meaningful dialogue at all. As a result, IDC accountability will continue to be a game of hot potato as long as data related to real causes remains obscured. Here is a sampling of some of the predominant viewpoints on that attribution analysis:

(a) Blaming the citizen-victim

Increasingly, reports and accounts from defrauded businesses cite vulnerable home user systems as being a major reason why criminals and miscreants are able to access, acquire, and use data to commit

129. *See* Press Release, Dep't of Justice, Prosecution Priorities for ID Theft Working Group 1, *available at* http://www.atg.wa.gov/uploadedFiles/Another/News/Press_Releases/2006/IDTheft-Priorities.pdf.

IDC.[130] The claims are that citizen-victims' negligence in practicing secure computing renders them a significant cause of the IDC problem.[131] Corporate-sponsored studies are quick to point out estimates of the significant number of home users' machines that are notoriously laden with malware, thus implicating users themselves as threat vectors into corporate databases.[132] A study by Morgan Stanley Consumer Banking alleged increasing fraud levels due in part to unsafe data handling and Internet practices. A Javelin study alleged that "consumer-controlled" unlawful acquisitions of identity data outpaced those by business seventy-nine to twenty-nine percent, respectively.[133] Not coincidentally, this report was funded by Visa, Wells Fargo and CheckFree Corporation, financial institutions which have a strong interest in championing the trustworthiness of online banking as well as shifting blame for any unreliability to citizen-victims so as to avoid the regulatory costs of responsibility for security breaches. Specifically, Javelin went on to pronounce: "[o]ur greatest vulnerability arises from information stolen by family, friends and in-home employees, those whom we trust most and allow the greatest access to our private information. There is no simple fix to this problemFalse".[134]

(b) Blaming institutions handling personal data –lack of incentives and accountability to safeguard.

This viewpoint maintains that IDC proliferates because companies are not effectively incentivized to prevent, detect and/or respond to IDC. This includes implementing more stringent data security safeguards, identifying breaches of identity data, and reporting fraud incidents. As

130. Dan Collins, *Home Internet Security is Woeful*, CBSNews.com, Oct. 25, 2004, http://www.cbsnews.com/stories/2004/10/25/tech/main651163.shtml.

131. Division of Supervision and Consumer Protection, *Cyber Fraud and Financial Crime Report* (Nov. 9, 2007), *available at* http://tinyurl.com/4dx4bg.

132. *See, e.g.,* Ed Skoudis, *Enterprise Security in 2008: Malware Trends Suggest New Twists on Old Tricks*, SEARCHSECURITY, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1294085,00.html (reporting that there are multiple botnets, each comprised of more than 1 million infected machines); Alexander Gostev, *Kaspersky Security Bulletin 2007: Malware Evolution in 2007*, VIRUSLIST, Feb. 26, 2008, http://www.viruslist.com/en/analysis?pubid=204791987 (claiming that 2007 was "the most virus-ridden year to date"); Nick Farrell, *One in Four US Computers Infected*, THE INQUIRER, June 2, 2008, http://www.theinquirer.net/gb/inquirer/news/2008/06/02/four-computers-infected.

133. *See* Javelin Report, *supra* note 117. *See also* Tom Pullar-Strecker, *Banks May Ease Line on Net Code,* THE DOMINION POST, July 9, 2007 (reporting that some banks in [country] are proposing to hold customers liable for losing all the money in their accounts up to the overdraft limit if they violate a "code of practices" which entails taking reasonable steps to protect their computers, including implementing "appropriate protective software" such as firewalls, ant-virus and anti-spyware, and patched operating systems).

134. Identity Theft 911, Maze of Contradictory Data Clouds Identity Theft Landscape, http://identitytheft911.org/articles/article.ext?sp=918 (last visited Apr. 11, 2009).

discussed more thoroughly in other sections, the discretion to report breaches and compromises to both victims and law enforcement, the allowance of security self-assessment standards, and the failure to recognize damages to individuals whose identities are breached, create a regime that supports the "antelope herd" mentality. Here companies know that the lion (a targeted assault for identity data) is ready to pounce, they just don't want to be the antelope unlucky enough to be picked off. So the strategy is to stick with the herd –implement just enough security so as to not appear reckless when the breach occurs and then underwrite the losses as a cost of doing business. To race ahead of the pack would mean increased costs from heightened security safeguards at the frontend, which does not necessarily translate into a competitive advantage in the savannah that is the marketplace. In the current market dynamic, racing ahead of the pack in this way would be regarded as a profit margin killer that would pose a formidable threat to institutional survival.

What are the manifestations that incentives and accountability for protecting data are lacking? In a macro sense, we can infer the breakdown via the near "breach-a-day" reports. The numbers speak for themselves, as highlighted by the top breaches since 2000:

1. TJX Companies, Inc.- 94,000,000 breached identities
2. American Express, Visa, Mastercard- 40,000,000
3. America Online- 30,000,000
4. U.S. Department of Veterans Affairs- 26,500,000
5. HM Revenue and Customs- 25,000,000.[135]

To drill down, familiar symptoms of lack of industry accountability include: weak identity authentication protections, deficient internal controls and ineffective auditing safeguards. For one, supporters of institutional accountability point to the fundamentally flawed authentication regimes used industry-wide by most organizations.[136] For example, some businesses send and/or store PII in clear-text, making it exponentially more susceptible to ID theft.[137] Also, industry relies almost exclusively on Secure Sockets Layer ("SSL") and single-factor authentication to conduct e-commerce with individual customers. While SSL protects

135. 10 Largest Data Breaches Since 2000, http://flowingdata.com/2008/03/14/10-largest-data-breaches-since-2000-millions-affected/10-largest-data-breaches-since-2000/ (last visited Oct. 16, 2008).

136. *See, e.g.,* Michael T. Goodrich, R. Tamassia & D. Yao, *Notarized Federated Identity Management for Web Services,* 16 J. COMPUTER SEC. 399, 418 (2008), *available at* http://www.cs.brown.edu/cgc/stms/papers/notarizedFIM.pdf.

137. *Id*. *See also* Posting of David Nevetta to InfoSecCompliance blog, Legally Mandated Encryption (Nov. 14, 2008), http://infoseccompliance.com/2008/11/14/legally-mandated-encryption/ (providing a summary of recent state laws passed mandating encryption of PII data transmitted across the Internet).

data in transit by encrypting it over the wire, it does not address vulnerabilities at the end points: the users' home systems and at the recipient business' databases.[138] There is widespread knowledge of the prolific threats posed by Trojan horses, keystroke loggers, and spyware on consumers' home systems, which allow thieves to compromise login access to corporate accounts.[139] Online financial fraud has grown so serious that the Federal Financial Institutions Examination Council, a government entity that establishes standards for banks, set deadlines for U.S. financial institutions to tighten authentication measures for accessing online accounts.[140] Yet, despite this known threat, businesses are implementing authentication protocols based on a lowest-common-denominator mentality, knowing that more rigorous measures are available but choosing not to apply them, absent a pressing incentive to incur the additional expenses.

For example, a recent data theft scam involving "click fraud" targeted Google searchers who clicked on paid ads, to which Google responded by implementing more stringent authentication for premium advertisers given the cost involved in implementing it for all of its member advertisers.[141] Certainly those who bear the costs of stronger security should reap the benefits, so those companies who pay for a measure should benefit. However, the reality is that by allowing a lowest-common-denominator authentication regime to exist, a digital interloper who breaches the corporate databases from a poorly authenticated account will compromise the same underlying data that some entities paid more to safeguard. Similarly, some banks choose not to implement more rigorous authentication controls which would reduce illegal use of pil-

138. *Id*.

139. Daniel Geer, Keynote Address at SOURCE Boston 2008 (Mar. 13, 2008), *available at* http://www.sourceconference.com/2008/sessions/dan-geer-keynote.html. Geer, one of the foremost computer security specialist's in the world, said:

> In the fall of 2006, I did some back of the envelope calculations that resulted in a guess that 15-30% of all desktops had some degree of external control present. I got a bit of hate mail over that but in the intervening months [Vinton] Cerf said 20-40%, Microsoft said 2/3, and IDG said 3/4. It doesn't matter which is right; what matters is that this changes a core feature of the ecosystem- and changing a core feature is the very definition of a punctuating event. In this case, it actually was not standing up a professional class of attackers any more than in the first go 'round it was a spike in the second derivative of the reported attack rate. What it was that a fundamental assumption of network security has now been breached and there is no putting it back together again.

Id.

140. CYBER SECURITY INDUSTRY ALLIANCE, FFIEC GUIDANCE ON AUTHENTICATION FOR ONLINE BANKING: GET THE FACTS 4 (2006), *available at* http://www.csialliance.org/publications/csia_whitepapers/CSIA_FFIEC_Get_Facts_November_2006.pdf.

141. *See Data Theft Scam Targets Google Searchers Who Click on Paid Ads*, INT'L HERALD TRIBUNE, Apr. 26, 2007, *available at* http://www.iht.com/articles/ap/2007/04/27/business/NA-TEC-US-Google-Paid-Ad-Scam.php.

fered identities for citizen customers while doing so for corporate customers based on cost considerations.[142]

One of a few industry-wide incentives to enhance security is the Payment Card Industry ("PCI") requirements. Previously companies who could afford to (large companies who have comparable security budget) simply paid a fine if they were found to be noncompliant with a statute. The TJX data breach stands as a hallmark illustration.[143] In theory, PCI put teeth behind the implementation of security standards under the threat that Visa or Mastercard could issue a death knell and deny them the ability to process cards, thus putting them out of business. However, it is dubious as to whether this is being enforced in any appreciable way. In fact, there is some evidence to support the contention that companies are manifestly not abiding by the PCI standards.[144]

A second, oft-cited symptom of a flawed incentive regime is the poor internal controls that allow trusted insiders to become a burgeoning threat vector in IDC. The FDIC reported that sixty-five to seventy percent of ID theft is committed with confidential information stolen by employees or participants in transactions or services.[145] In 2006, a CSO Magazine study found that when businesses could identify sources of attacks on consumer records, fifty-six percent were attributable to insiders.[146] Symantec similarly found that theft or loss of an employee's computer accounted for fifty-four percent of identity theft breaches in a

142. Remarks at the FTC Authentication Workshop (Fall 2007) (on file with author).

143. *See* Jenn Abelson, *Breach of Data at TJX is Called the Biggest Ever,* BOSTON GLOBE, Mar. 29, 2007, at A1, *available at* http://www.boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever/. *See also* Evan Schuman, *What Was Behind the TJX Settlement?*, EWEEK, Sept. 24, 2007, http://www.eweek.com/c/a/Enterprise-Applications/What-Was-Behind-the-TJX-Settlement/. Schuman reported that:

> When TJX announced Sept. 21 that it had worked out a settlement for all of the consumer lawsuits that had been filed against it, it provided an anticlimactic ending to much of this data breach saga. But in many ways, this resolution—with a settlement offer that will cause TJX very little material pain—was inevitable. Despite the background of the most massive data breach in retail history, where credit card data of some 46 million consumers fell into unauthorized hands, *TJX had virtually nothing to fear* from the U.S. judicial system.

Id. (emphasis added).

144. *See* Division of Supervision and Consumer Protection: *Cyber Fraud and Financial Crime Report*, http://blog.washingtonpost.com/securityfix/FDIC%20INCIDENT%20REPORTR2Q07r.htm (last visited Oct. 16, 2008).

145. FED. DEPOSIT INS. CORP., PUTTING AN END TO ACCOUNT-HIJACKING IDENTITY THEFT 10 (2004), *available at* http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

146. Press Release, CSO Magazine, Survey Show E-Crime Incidents are Declining Yet Impact is Increasing (Sept. 6, 2006), *available at* www.cert.org/archive/pdf/ecrimesurvey06.pdf. *See also* Jeremy Kirk, *Hackers Selling IDs for $14, Symantec Says,* INFOWORLD, Mar. 19, 2007, http://www.infoworld.com/article/07/03/19/HNhackerssellids_1.html; Tom Young, *Security Threats are Starting to Merge*, COMPUTING, Mar. 19, 2007, *available at* http://www.computing.co.uk/computing/news/2185766/threats-begin-blend; Brian Krebs, *Stolen Identi-*

six-month period between July and December of 2006.[147] To round it out, Javelin reported similar threats emanating from the citizen-victim contingent.[148] And finally, the FDIC Computer Intrusion Report leaked to *The Washington Post*, and published by that entity on March 5, 2008 noted that ". . .lending-related insider abuse caused the most losses followed by theft from depositor accounts."[149] These assertions that the insider threat to identity information is significant and increasing support a reasonable inference that companies are not incentivized to implement preventative controls that would adequately address this threat.

A third familiar species of the corporate attribution theory points to the lack of incentives and accountability for ensuring the quality of the data linking persons to fraudulent transactions.[150] This dimension of IDC is by some accounts more nefarious than the direct leaking of PII into the criminal marketplace, or even the dereliction of security controls, insofar as it spawns a lineage of inaccurate information within the legitimate marketplace. Financial institutions are not liable for sending erroneous information to credit reporting bureaus based on fraudulent transactions.[151] In other words, there is no accountability for reporting the transactions of identity thieves as the transactions of consumer victims. In fact, industry has been the staunchest opponent to the consumer credit freeze laws, which provide citizens with one of the few tool tools to prevent ID theft.[152] Furthermore, there is allegedly complicity if not outright collusion with information intermediaries such as credit reporting bureaus and data brokers.[153] These organizations have no direct

ties Sold Cheap on the Black Market, WASHINGTONPOST, SECURITY FIX, Mar. 19, 2007, http://blog.washingtonpost.com/securityfix/2007/03/stolen_identities_two_dollars.html.

147. SYMANTEC, SYMANTEC INTERNET SECURITY THREAT REPORT: TRENDS FOR JULY-DECEMBER 06 5 (2007), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf.

148. *See* Javelin Report, *supra* note 108.

149. *See* Division of Supervision and Consumer Protection: *Cyber Fraud and Financial Crime Report*, http://blog.washingtonpost.com/securityfix/FDIC%20INCIDENT%20REPORTR2Q07r.htm (last visited Oct. 16, 2008).

150. Quality here refers to core attributes of accuracy, completeness, authenticity and timeliness.

151. Bruce Schneider, *Mitigating Identity Theft*, CRYPTO-GRAM NEWSLETTER, Apr. 15, 2005, http://www.schneier.com/crypto-gram-0504.html#2. Countering claims that this liability scheme will not work, Schneider points out that credit card companies have managed to thrive despite being held accountable for all but the first $50 of fraudulent transactions. *Id*. This is an illustration where the liability has incentivized them to develop and deploy security technologies to detect and prevent fraudulent transactions. *Id*.

152. Fair and Accurate Credit Transactions Act, Pub. L. No. 108-159, 117 Stat. 1952 ("FACTA") (codified at 15 U.C.S. § 1601 (2003)). FACTA did provide some relief to the consumer (at a price, of course). *See also* NAT'L CONSUMER LAW CTR., ANALYSIS OF THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003 (2003), *available at* http://www.consumerlaw.org/issues/credit_reporting/nclc_analysis.shtml.

153. See *infra* note 161.

relationship or duty to citizen-consumers, so from their view ensuring data quality and remediating incorrect data imposes costs for which there is no Return on Investment ("ROI").[154]

According to Leonard Bennett, "[t]he CRAs simply parrot whatever they receive from the furnisher. At the same time, the furnishers are relying heavily on the fact that there is no private cause of action under Section 1681s-2(a) and no standard for the furnisher investigation under Section 1681s-2(b). Nearly all institutional furnishers have the same procedures."[155] Further, as Jeff Sovern notes in his article, *The Jewel of Their Souls: Preventing Identity Theft Trough Loss Allocation Rules*:[156]

> credit bureaus may actually have disincentives to take steps to prevent identity theft. . . If they can develop mechanisms to reduce the incidence of identity theft, they can market those mechanisms separately for an additional fee. If, on the other hand, they make those mechanisms available without extra charge, they give up potential income.

The New York Times reinforced this dynamic in an article stating that "the biggest beneficiaries from identity theft have been the three credit bureaus" and that the credit-monitoring services sold by the big three credit bureaus are nearly a billion-dollar business.[157] This complicity criticism has also extended to the United States government as it relates to unclaimed payments made into the Social Security and Medicare programs. Stolen identity information, including SSNs, is used to obtain employment for illegal and undocumented immigrants. The Social Security withholdings collected from workers using false or unverified identification go into the Earnings Suspense File.[158] It is estimated that hundreds of billions of dollars over the past fifty years have flowed into this file from unidentified or misfiled SSNs resulting from ID theft.[159] This fact buttresses the notion that ID theft has incentivized complicity at worst, and benign neglect at best within the government.

---

154. That is, as discussed in the next section, unless data quality can be offered up as a service upon which to profit.

155. *Testimony Before Subcomm. on Financial Institutions and Consumer Credit of the Comm. on Financial Services Regarding Fair Credit Reporting Act: How it Functions for Consumers and the Economy*, 108th Cong. 8 (2003), *available at* http://financialservices.house.gov/media/pdf/060403lb.pdf (testimony of Leonard A. Bennett on behalf of National Association of Consumer Advocates).

156. Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules,* 64 U. PITT. L. REV. 343, 362 (2003).

157. *See* Eric Dash, *Protectors, Too, Gather Profits From ID Theft*, N.Y. TIMES, Dec. 12, 2006, at 28, *available at* http://www.nytimes.com/2006/12/12/business/12credit.html.

158. *See, e.g.*, Julia Preston, *After Iowa Raid, Immigrants Fuel Labor Inquiries,* N.Y. TIMES, Jul. 27, 2008, at 1, *available at* http://www.nytimes.com/2008/07/27/us/27immig.html?pagewanted=2&_r=1.

159. Martin H. Bosworth, *Persecution of Immigrant Workers Won't Stop Identity Theft*, Dec. 22, 2006, http://www.consumeraffairs.com/news04/2006/12/swift_raids.html.

How has this framework of insufficient incentives and mutable accountability been molded? While previous sections address the pathology of IDC, it bears repeating because it is argued that attribution for the IDC problem should fall significantly on the shoulders of the organizations managing PII. One view is that the policies promoting the instant credit financial regime not only lower the barriers for fraudsters seeking economic gain, but also incentivize companies to issue more credit at the front end rather than instituting more rigorous identity data protections at the backend. This is patently obvious when one compares the current ease with which one can obtain credit with virtually no identity authentication, versus the time and labor required to prove identity post-fraud in order to remediate losses or put a hold or freeze on one's credit.[160] In other words, there is no legislative stick or financial carrot to incentivize business, as PII intermediaries, to effectively prevent ID theft or to limit the dissemination of or ameliorate the consequences of inaccurate data. One might conclude that to do so would undercut the demand for their growing products and services sector that focus on IDC issues.[161] There's no better way to assure demand for a product solution than by perpetuating the underlying need.

(c) Changes in reporting and increased awareness of the problem

A third IDC attribution theory maintains that ID theft is less about significant acts or omissions by either citizens, institutions, or perhaps even criminals than it is an artifact of changes in awareness and reporting. Since laws prohibiting ID theft are less than ten years old, the claim is that we are experiencing the syncing of our social values and institutional controls –laws and practices. This can be likened to domestic violence, where statistics on a previously under-reported social problem-turned-crime seemed to skyrocket relative to a non-existent baseline of reporting practices. From the law enforcement perspective, number jumps can be explained by changes in recording.[162] Since ID theft is often associated with other financial and drug-related crimes, it was not always recorded or charged as a separate offense.[163] This is true as well with the addition of ID theft-specific offenses which have spawned with the new laws, providing the possibility that previous ID thefts may have been retrofitted into broad fraud charges. Also, from an aggregate, nationwide perspective, not all LE agencies cooperated with the national

160. *See* Nancy J. Perry, *How to Protect Yourself from the Credit Fraud Epidemic*, Aug. 1, 1995, http://money.cnn.com/magazines/moneymag/moneymag_archive/1995/08/01/205197/index.htm.

161. *See* Tim Wilson, *Amid Confusion, Market for ID Theft Services Grows,* DARKREADING, Dec. 19, 2007, http://www.darkreading.com/document.asp?doc_id=141762.

162. *See* NEWMAN, *supra* note 42, at 59.

163. *Id.*

reporting standards, making completeness of those numbers a moving target.[164]

Regardless of the truth of these claims, the very reasons supporting the increased reporting theory are based on insufficient ID theft data. Likewise, whether and to what degree ID theft can be attributed to citizens, institutions, or reporting changes will forever be a game of hot potato or a breeding ground for social and legal fiction until more empirical IDC data is obtained.

ii. Damages Conundrum: Fictions Created and Perpetuated in the Wake of the Data Breaches.

The next defective, second-order analysis resulting from the dearth of IDT data is the damages assessment, and it falls along two axes. First, damages as "legal fictions" refers to damages in the traditional legal sense, which is to say judicially-recognized, recoverable damages. Second, damages as "social fictions" denotes IDT damages in the familiar public vernacular –the aggravation and stress felt by IDT victims. For example, this would include the costs associated with time spent clearing up problems resulting from others wrongfully using PII. This is recognized by the public as damage resulting from ID theft, yet such damages might not be deemed recoverable under any prevailing legal theory.

(a) Current Posture on Damages: Theories and Legal Fictions

Humans find it necessary at times to create legal and/or social fictions which provide the illusion of control in the face of "information chaos." The fictions in question serve as a coping mechanism, and because of the indeterminism associated with IDC, damages jurisprudence in data breach cases is an exercise in weaving legal fictions. This legal-fictioning serves two purposes. One, it defines boundaries around novel issues presented by IDC and data breaches within which the efficient administration of justice can occur. Second, it uses the judiciary as a firewall to institutionalize the restriction of liability risk for those entities that profit from the accumulation and manipulation of PII in the form of digital data.

The landscape formed from damages analysis, post-wrongful PII acquisition, is a major hurdle to accurately scoping IDT, which ultimately contributes to misinformed policy related to IDT. By damages analyses, we include the following determinations: when actual injury occurs, what and when damage is done, and when individuals' information has been stolen by those who intend a harmful act with the information in

164. UNITED STATES GENERAL ACCOUNTING OFFICE, IDENTITY FRAUD: INFORMATION ON PREVALENCE, COST, AND INTERNET IMPACT IS LIMITED 22-23 (1998), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO/GGD-98-100BR.

question. *Stollenwerk v. Tri-West Health* can be cited as the first data breach case to address the issue of damages under a negligence claim in the wake of a data breach.[165] The vast majority of civil litigation[166] decided in the wake of a data breach can be seen as *Stollenwerk* progeny in that courts have in large measure consistently embraced the lack of actual injury holding emanating from *Stollenwerk*, which in turn leads to finding no recoverable damages or loss.[167] Therefore, companies suffering the data breach are not being held liable.

Civil laws require an articulation of damage, loss, and harm prior to filing a civil claim.[168] This can be an onerous and capricious challenge for victim-plaintiffs in the civil context. The plaintiff, as illustrated in our analysis of *Key v. TRW*, has to prove that an actual injury occurred as a result of the data breach.[169] Otherwise, recoverable damages and loss become a moot point.

This hurdle is made all the more challenging by the dynamics of class action lawsuits, which are especially attractive given the features of data breaches (i.e., large numbers of similarly situated plaintiffs). Specifically, class action suits place substantial financial pressures on plaintiffs' attorneys to move quickly in the wake of perceived tort or breach of contract.[170] However, what are commonly thought of as dam-

165. Stollenwerk v. Tri-West Health Care Alliance, No. CIV 03-0185-PHX-SRB, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. 2005).

166. *See, e.g.*, Forbes v. Wells Fargo, 420 F. Supp. 2d 1018 (D. Minn. 2006); Giorando v. Wachovia Sec., Civ. No. 06-476JBS, 2006 WL 2177036, at *1 (D.N.J. July 31, 2006); Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. Civ. 05-668, 2006 WL 288483 (D. Minn. Feb. 7, 2006).

167. Lack of actual damages has also been the stumbling block under other theories of recovery besides negligence. Further, in the pre-notification era where the fact scenario giving rise to an exposure of PII was not necessarily from a database breach, actual damages posed a barrier. For instance, courts have found no recovery under the Federal Privacy Act for disclosure of a SSN. *See, e.g.*, Doe v. Chao, 306 F.3d 170 (4th Cir. 2002) (noting that while Buck Doe had sworn in an affidavit that he was "embarrassed", "degraded", and "devastated," by the disclosure of his SSN, this was insufficient to raise an issue of fact). He did not allege the requisite manifestations of emotional distress, such as "medical or psychological treatment," "purchase of medications," and "physical consequences" to meet the requirement for proving actual damages under the statute. *Id*.

168. *See* Lowe v. Philip Morris USA, Inc*.,* 142 P.3d 1079 (Or. Ct. App. 2006). Although plaintiff claimed that she had a "significantly increased risk of developing lung cancer," the court observed that she did not claim that her risk of future harm was "all but certain" or even probable. *Id*. at 1081. The court held that allowing a claim "for a mere increase in the possibility of future harm" would be inconsistent with the "fundamental premise" of Oregon law "that the plaintiff must have suffered actual, physical harm." *Id*. The court concluded that actual harm "is the sine qua non of negligence liability." *Id*. at 1088.

169. *See* Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006).

170. The first to file is often, but not always, deemed by the court to be the lead lawyer in the suit. This equates to larger fees if the case is successful. While this "first to file" dynamic was deemed to be eliminated by the federal, so called, Class Action Fairness Act of

ages resulting from the theft of data often have a latency, and thus may take a substantial amount of time to manifest themselves.[171] If the case is adjudicated prior to the revelation of the misuse, the judge may reason that she has no choice but to dismiss the case. Given the influence that *Stollenwerk* has wielded on the judicial recognition of identity theft, and the ramifications of the judicial posture, further dissection is in order.

(i) Stollenwerk v. Tri-West Health Care Alliance.[172]

Plaintiffs Stollenwerk, DeGratica, and Brandt sued Tri-West for "negligently fail[ing] to secure their personal information maintained on Tri-West's computers."[173] Plaintiff's information had been stolen as a result of an on-site burglary at Tri West.[174] The thieves broke in and stole the computer servers that held the information in question.[175] Plaintiffs alleged different grounds for their respective causes of action. Stollenwerk and DeGratica claimed they were entitled to recover damages for the costs incurred as a result of having to obtain heightened credit monitoring services to protect themselves against the fraudulent use of their pilfered PII.[176] Plaintiff Brandt, on the other hand, claimed damages allegedly resulting from the burglary.[177] These damages came

---

2005, the authors can still find, and do find, class action trial lawyers who tell them this is not accurate. They point out that the first to file can lead to the 'first to settle,' and the first to settle means you can draw in more class action plaintiffs. *See* Wikipedia, *Class Action Fairness Act of 2005*, http://en.wikipedia.org/wiki/Class_Action_Fairness_Act_of_2005 (as of Mar. 11, 2009, 14:11 GMT).

171. "76% of all identity theft is discovered before 24 months after the theft. *Only* 12% is discovered more than 48 months after the theft." Bell v. Acxiom Corp. 2006 U.S. Dist. LEXIS 72477 at *4 n.22 (E.D. Ark. 2006) (citing FEDERAL TRADE COMMISSION IDENTITY THEFT VICTIM COMPLAINT DATA 2005 11 (2006), http://www.ftc.gov/sentinel/reports/idt-annualoverall-figures/idt-cy2005.pdf) (emphasis added). Note that one survey done by the Chubb Insurance Group estimated that one in five Americans was subject to ID theft in the year 2005. *Survey: One in Five Americans Have Been Victims of Identity Fraud*, INS. J., July 8, 2008, *available at* http://www.insurancejournal.com/news/national/2005/07/08/57054.htm. So, based on that survey, the "only" referred to by the court might be in the tens of millions, depending on the parameters of the survey.

172. Stollenwerk v. Tri-West Health Care Alliance, No. CIV 03-0185-PHX-SRB, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. 2005), *aff'd in part, rev'd in part*, 254 Fed. Appx. 664 (9th Cir. 2007).

173. *Id.* at 665.

174. *Stollenwerk*, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. 2005). Plaintiffs claimed Tri-West took no steps in the weeks following the first burglary to upgrade their defenses for the building. *Id*. at *2.

175. It is not clear from the court opinion whether anything else was taken in the burglary. *Id.*

176. *Stollenwerk*, 2005 U.S. Dist. LEXIS 41054 at *6.

177. *Id*. at 1 ("This matter arises out of the burglary of Defendant TriWest Healthcare Alliance's ("Triwest") corporate office on December 14, 2002.").

in the form of fraudulent use of his PII to open and/or attempt to open credit accounts.

In both cases the federal district court denied the claims. Plaintiffs Stollenwerk and DeGratica compared the theft of the information and possible resulting harm in the future to toxic tort cases where medical monitoring for future harm was held to be necessary as a result of the exposure.[178] Plaintiffs argued that in the wake of having their PII stolen, something akin to medical monitoring was called for (i.e. credit monitoring services and the cost to obtain them should be recoverable losses).

The court rejected this argument. It did acknowledge that in some cases data theft is not "entirely dissimilar" from "exposure to toxic substances and unsafe products," but felt that for other reasons it was not necessary to reach a decision on that issue in the present case.[179] That "important distinction" was based on the rationale that toxic tort and products liability cases raise issues of public safety which, the court noted, are not present with data breach cases.[180] Further, the court seemed to be concerned with the lack of quantifiable metrics that might demonstrate a relationship between heightened credit monitoring services and any potential impact those services may have on reducing the risk of future damages from misuse of the personal data.[181]

Unintentionally adding insult to injury, the court held that while plaintiff Brandt did indeed suffer some actual injury as a result of his data being stolen, namely that credit accounts were actually opened in his name in the wake of the theft of the data, the causal relationship between the theft and the subsequent opening of the accounts was too attenuated, and therefore lacked the elements necessary to establish a cause of action.[182] The court reasoned that while Brandt did provide enough admissible evidence to establish a "reasonable inference" that the burglary was the direct cause of the opening of the subsequent unauthorized credit accounts, the evidence was simply a result of "speculation and conjecture"[183] on the part of the plaintiff.[184]

178. As did plaintiffs in Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006).

179. *Stollenwerk*, 2005 U.S. Dist. LEXIS 41054 at *9-10.

180. *Id.*

181. *Id*. at *14.

182. *Id.* at *20-21.

183. *Id.* at *20.

184. It should be noted that 9th Circuit Court of Appeals overturned this part of *Stollenwerk,* 254 Fed. Appx. 664 (9th Cir. 2007) (holding that plaintiff Brandt's claim could go forward on the grounds that a causal relationship between the data breach, and the subsequent misuse of the data had been established). Unfortunately, for reasons not specified the opinion was declared an unpublished opinion, meaning it has no precedential value and therefore cannot be cited as authority for future cases.

(ii) Stollenwerk Progeny and Analogous Law.

Most courts dealing with fact patterns similar to *Stollenwerk* have followed its holding, sometimes citing it directly and other times simply adopting the spirit of *Stollenwerk*.[185] We examine several of these to highlight the trend in judicial opinions.

Kupla v. Ohio University is a case where the *Stollenwerk* holding predominated but was not cited.[186] *Kupla's* fact pattern is similar in that data was taken, albeit as a result of a hack and not a burglary. The Ohio University system was subject to an ongoing hack that lasted approximately one year. Kulpa was one of the students who claimed that as a result of the hack he suffered a heightened risk of ID theft, among other claims.

Defendant Ohio University, citing the holding in *Kahle v. Litton Loan Servicing*[187] and *Key v. DSW Inc.*, asked for the case to be dismissed for failure to state a claim. Both of these cases cited by the *Kupla* court favorably reference the *Stollenwerk* holdings. With one notable exception,[188] the *Kulpa* court ruled, consistent with the *Stollenwerk*, that the threat of "future injury is not an actual or imminent[189] injury."[190] Therefore the costs for credit monitoring services were not recoverable, as per the *Stollenwerk*, *Kahle* and *Key* cases. This, we suggest, is same rationale proffered to dismiss most if not all of the data breach notification cases brought in the United States.

Thus far, courts have been relatively consistent in not recognizing what is an almost organic, or inherent delay between unauthorized access and exposure of identity artifacts and their manifested misuse by a

185. By similar patterns we mean "data theft," whether as a result of burglary, a hack, a lost laptop, etc.

186. *See* Kulpa v. Ohio Univ., No. C2006-04202 (Ohio Ct. Cl. Sept. 13, 2007), *available at* http://www.cco.state.oh.us/scripts/ccoc.wsc/ws_civilcasesearch_2007.r?mode=5&CaseNo=200604202.

187. Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705 (S.D. Ohio 2007).

188. Kulpa v. Ohio Univ., No. C2006-04202, at ¶5 (Ohio Ct. Cl. Sept. 13, 2007), *available at* http://www.cco.state.oh.us/scripts/ccoc.wsc/ws_civilcasesearch_2007.r?mode=5&CaseNo=200604202 (emphasis added) (citing *Kahle*, the court noted that "without direct evidence that the information was accessed or specific evidence of identity fraud this Court cannot find that the cost of obtaining credit monitoring to amount to damages in a negligence claim."). One would be hard pressed to explain how hacking into a system where Kupla's information was—as the fact pattern makes that occurred—is not "direct evidence that the information was accessed". And yet that is exactly what the *Kupla* court found. So, the *Kahle* court, cited in *Kupla* was actually rejecting *Stollenwerk* on the issue of credit monitoring. It could be grounds for recovery of damages. Instead, the court scrambled to come up with a causation issue by twisting the definition of access.

189. We think many of elements of this definition match the situation *Kupla* et al. were facing.

190. *Kulpa*, No. C2006-04202 (citing Key v. DSW, Inc., 454 F. Supp. 2d 684 (S.D. Ohio 2006)).

third party.[191] Instead, courts have for the most part insisted on requiring current, actual harm in order to meet the damages element of the various breach-related causes of action.[192] We suggest that this "injury in fact" interpretation may be unduly narrow at best and factually incorrect at worst.

A comparative analysis of another legal domain where actual injury (in the legal sense) has been an issue up may be instructive. Insurance law has confronted an analogous issue, delayed manifestation illness. The question at issue in *Keene Corp. v. Insurance Co.*[193] was how to establish standards to measure when an exposure to a harmful substance– asbestos– manifests itself in actual, legally recognizable injury –mesothelioma.[194] We duly acknowledge the distinction between claims in an insurance context versus a tort context in that they involve con-

191. The exception is *Bell v. Mich. Council 25*, No. 246684, 2005 Mich. App. LEXIS 353, (Mich. Ct. App. Feb. 15, 2005). The court held that:

> However, with the advancements in technology, holders of such information have had to become increasingly vigilant in protecting such information and the security measures enacted to ensure such protection have become increasingly more complex. As demonstrated by the problems plaintiffs' faced after their identities had been appropriated, the severity of the risk of harm in allowing personal identifying information to be taken to an unsecured environment is high. The instant plaintiffs were very fortunate regarding the limited extent of the fraud perpetrated using their identities. But it is the potential severity of the risk, not the actual risk encountered, that must be considered in deciding to impose liability.

Id. at *3-14 (emphasis added)). The court is rejecting the tone, if not the specific on point holding in *Stollenwerk*.

192. As we believe *Pisciotta v. Old Nat'l Bancorp* makes clear:

> Finally, without Indiana guidance directly on point, we next examine the reasoning of other courts applying the law of other jurisdictions to the question posed by this case. *Allstate Ins. Co.*, 392 F.3d at 952. In this respect, several district courts, applying the laws of other jurisdictions, have rejected similar claims on their merits. In addition to those cases in which the district court held that the plaintiff lacked standing, a series of cases has rejected information security claims on their merits. Most have concluded that the plaintiffs have not been injured in a manner the governing substantive law will recognize. *See, e.g.*, *Kahle v. Litton Loan Servicing, LP*, 486 F. Supp. 2d 705, 712-13 (S.D. Ohio 2007) (entering summary judgment for the defendant because the plaintiff had failed to demonstrate an injury); *Guin v. Brazos Higher Educ. Serv. Corp., Inc.*, 2006 U.S. Dist. LEXIS 4846, 2006 WL 288483 (D. Minn. Feb. 7, 2006) (unpublished) (same); *Stollenwerk v. Tri-West Healthcare Alliance*, 2005 U.S. Dist. LEXIS 41054, 2005 WL 2465906, at *5 (D. Ariz. Sept. 6, 2005) (unpublished) (granting summary judgment for defendants because the plaintiffs had failed to provide evidence of injury); *see also Hendricks v. DSW Shoe Warehouse*, 444 F. Supp. 2d 775, 783 (W.D. Mich. 2006) (dismissing an action where "[t]here is no existing Michigan statutory or case law authority to support plaintiff's position that the purchase of credit monitoring constitutes either actual damages or a cognizable loss").

Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639 (7th Cir. 2007). The vast majority of case law on the data breach class actions has required, for a finding of recoverable damages, a finding of, as the *Pisciotta* court noted, "a harm that the law is prepared to remedy." *Id.*

193. Keene Corp. v. Ins. Co. N. Am., 667 F.2d 1034 (D.C. Cir. 1981).

194. *Id*. at 1038 n.3.

tractual issues rather than negligence issues, respectively. However, the comparative analogy is still instructive to view how some courts have grappled with a process of marking a moment in time when the occurrence of injury is recognized in a legal sense for purposes of recovering damages.

For instance, the Fifth and Sixth Circuits have held that state courts could adopt an "exposure" theory.[195] When dealing with injuries related to asbestos, the "exposure" theory holds that the first time the asbestos fibers were deposited into the lungs the actual injury had occurred, however long it may have taken to manifest itself upon the victim.

On the other hand, other jurisdictions have held that state courts could adopt a "manifestation" theory when the first confirmation is found that exposure had matured to a disease.[196] The *Keene* court rejected

---

195. *See* Ins. Co. of N. Am. v. Forty-Eight Insulations, 633 F.2d 1212, 1281 (6th Cir. 1980). The Court noted that:

> Aside from this, however, we believe that the policy language itself is best construed along the lines of the exposure theory. We need only look at the definition of "bodily injury" in the policy. Bodily injury is defined as "bodily injury, sickness or disease . . ." It is tautological that bodily injury can be "bodily injury" and is not necessarily just a "disease". The medical evidence is uncontroverted that "bodily injury" in the form of tissue damage takes place at or shortly after the initial inhalation of asbestos fibers. Thus, it requires only a straightforward interpretation of the policy language for us to adopt the exposure theory. Indeed, for insurance purposes, courts have long defined the term "bodily injury" to mean "any localized abnormal condition of the living body." See Appleman, Insurance Law and Practices § 355 (1965).

Id. *See also* Porter v. Am. Optical Corp., 641 F.2d 1128, 1145 (5th Cir. 1981). Held:

> We might prolong this already lengthy opinion by paraphrasing or rephrasing the Sixth Circuit opinion. We are content to say that we agree with its reasoning and result. Under the terms of the policies presently before us we reject the "manifestation" theory. We accept the "injurious exposure" theory and the logically consequent rule of proration of liability for insurance carriers who were on the coverage while the injured party was exposed to the asbestos hazards which resulted in illness and death.

Id.

196. *Keene Corp*., 667 F.2d at 1042-43. The court observed that:

> INA, Liberty, and Aetna advance the "manifestation" theory of coverage. They argue that coverage is triggered only by the manifestation of either asbestosis, mesothelioma or lung cancer. They assert that their interpretation of the contracts is supported by the ordinary meaning of the terms "bodily injury, sickness or disease." They claim the "bodily injury" does not occur until cellular damage advances to the point of becoming a recognizable disease. INA and Liberty rely on cases in other areas of the law — workmen's compensation, health insurance coverage, and statutes of limitation — that support their interpretation of the term "injury." E.g., Travelers Insurance Co. v. Cordillo, 225 F.2d 137 (2d Cir.), cert. denied, 350 U.S. 913 (1955) (workmen's compensation), cited in Liberty's brief at 42-44 and INA's brief at 28; Reiser v. Metropolitan Life Insurance Co ., 262 App.Div. 171, 28 N.Y.S.2d 283 (1941) aff'd, 289 N.Y. 561, 43 N.E.2d 534 (1942) (health insurance), cited in Liberty's brief at 45 and INA's brief at 26; Urie v. Thompson, 337 U.S. 163 (1949) (statute of limitations), cited in INA's brief at 27.

Id.

both these theories on the grounds that in the context of asbestos-related disease, the terms "bodily injury," "sickness" and "disease," standing alone, simply lack the precision necessary to identify a point in the development of a disease at which coverage is triggered.[197] Finally, the District of Columbia Circuit has held that states could adopt a "multiple trigger" theory[198] and Pennsylvania state courts[199] have, in fact, adopted a multiple trigger theory.

The "multiple trigger" theory in particular might have special relevance to ID theft and data breach jurisprudence. There is much in Judge Patricia Wald's concurrence in *Keene* that has relevance for victims whose data has been stolen in a data breach cases.[200] Judge Wald opined in reference to the "multiple trigger" rational:

> The approach taken in the panel opinion here is different from the approaches of other courts in two significant respects. First, it defines the "injury" that triggers insurance coverage not merely as exposure to asbestos fibers or manifestation of the symptoms of asbestosis, mesothelioma or lung cancer, but also—at least in the case of asbestosis—as the *process* by which the victim's body resists, adapts, and tries to accommodate itself to a foreign matter—aprocess, which we understand from the medical testimony elicited at trial, is a major, if not primary, factor in the development of asbestosis. In short, the "injury" is taking place every year that the asbestos fiber remains in situ until tissue damage in the lungs is significant enough to be detected by X-rays or to produce symptomatic effects of asbestosis, mesothelioma or lung cancer. I agree with this more comprehensive definition of "injury," encompassing the period from initial exposure to manifestation, because it comports with what we know *and do not know* about the etiology and progress of the diseases. *This process-oriented definition not only provides a flexible*

197. *Id*. at 1043.

198. Eli Lilly & Co. v. Home Ins. Co., 794 F.2d 710, 716 (D.C. Cir. 1986). The court noted that:

> Thus, contrary to the contention of appellants, *see* Joint Post-Certification Supplemental Memorandum of Defendants-Appellants filed November 27, 1985 at 16, the Indiana court apparently did not think extrinsic evidence should be used to determine the character of such "reasonable expectations." Instead the court seemed to have determined the content of such expectations — the multiple trigger thesis — as a matter of law.

Id.

199. J.H. France Refractories Co. v. Allstate Ins. Co., 534 Pa. 29, 37 (Pa. 1991). Held:

> In similar fashion, the Superior Court reached the conclusion that the term "bodily injury" also encompasses the progression of the disease throughout and after the period of exposure until, ultimately, the manifestation of recognizable incapacitation constitutes the final "injury," and that these stages in the pathogenesis of asbestos- and silica-related diseases also trigger the liability of J.H. France's insurance carriers. We find no error in this analysis and conclusion. The insurance policy language and the evidence of the etiology and pathogenesis of asbestos-related disease compel us to reach this result.

Id.

200. *Keene Corp*., 215 U.S. App. D.C. at 56.

> *formula for adjudicating the legal issues associated with asbestos-related diseases, but also sets a useful precedent for other product-exposure injuries, as of yet unknown in origin*. Further, the more comprehensive definition will give much needed certainty to the insurance industry, currently rent asunder by advocates of exposure and manifestation, whose fluctuating positions often depend upon their economic interests in a particular case, and by differing judicial rulings which seem to depend at least partially upon the equities of each case[201]

While it is intimated that the risk of ID theft equates to the grave hazards of mesothelioma or lung cancer, it is advocated that borrowing the latter's "process-oriented" definition of injury is useful in IDT data breach cases, particularly since it is an undeveloped area of the law as well as a little understood area of commerce and finance. Only very recently, and with a notable lack of reliable data, has society begun to understand how PII data is used and misused in our society. Keeping in mind Judge Wald's caution about what we know "*and do not know* about the etiology and progress. . ."of disease, the courts might blow a slightly less certain note on their respective trumpets with regard to damages analyses in data breach cases.

This is especially so at a time when society has moved to risk based pricing schemes which are predicated on timely access to accurate data, to say nothing of our increasing reliance on database analytics which are increasingly the gateway to citizens' opportunity to transact, travel and conduct commerce without undue interference.[202] As Judge Wald recounted:

> [T]his is a case of first impression and, irrespective of how it is resolved, requires a "leap of logic," from existing precedent, for it concerns diseases about which there is no medical certainty as to precisely how or when they "occur." We do know the prerequisite—exposure to asbestos fibers—and the symptoms that manifest themselves, generally too late for effective treatment. What happens in between is still something of a mystery; why does one exposed person fall victim to the diseases while another does not?[203]

Moving from insurance law back to IDT, *Pisciotta v. Old National Bancorp* is the one data breach case that comes closest to marshalling all the previously highlighted standards: exposure, multiple trigger, and diagnosis/presumptive present harm.[204] This case engages in one of the most intelligible discussions of the damages analysis of when ID Theft

---

201. *Id*. at 1057-58 (emphasis added).

202. *See* Wikipedia, *Risk-based Pricing*, http://en.wikipedia.org/wiki/Risk-based_pricing (as of Nov. 19, 2008, 13:12 GMT).

203. *Keene Corp*., 667 F.2d at 1057.

204. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. 2007).

occurs.[205]

Pisciotta was a customer of the Old National Bancorp. He used the bank's online banking service. The bank's website was hacked and the PII in question was stolen. Plaintiffs filed a class action negligence lawsuit claiming actual injury from the theft of the data, and damages for credit monitoring costs incurred to prevent further harm from "future" ID theft.[206] While Indiana did not have a Data Breach notification statute at the time of the hack and the subsequent filing of the complaint, the state did pass one shortly thereafter.[207] The court, while acknowledging the Indiana statute was not "directly applicable to the present dispute," nonetheless used it to guide its decision.[208]

The court found that the statute provided no private right of action, nor did it create a duty on the part of the breached entity "to compensate affected individuals for inconvenience or potential harm to credit that may follow."[209] The plaintiffs maintained that "the statute is evidence that the Indiana legislature believes that an individual *has suffered a compensable injury at the moment* his personal information is exposed because of a security breach."[210] Indeed, the court indicated that they thought this was the challenge they face in *Pisciotta* when they noted that:

> We must determine whether Indiana would consider that the harm caused by identity information exposure, coupled with the attendant costs to guard against identity theft, constitutes an existing *compensable injury and consequent damages* required to state a claim for negligence or for breach of contract.[211]

In articulating this challenge, the *Pisciotta* court indicated there were two distinct, but perhaps related, elements to the challenge.[212] First, there is the issue of "exposure." The second element was the "costs" associated with preventing future ID theft. These two elements,

---

205. The discussion is couched in murky terminology, again, at times, unstated, regarding what actual injury, if any, occurs at the moment the data in question is transferred, in an unauthorized manner by someone intent on using in an unlawful manner.

206. Plaintiffs filed a breach of contract action as well.

207. Ind. Pub. L. 125-2006, § 6 (Mar. 21, 2006) (codified as IND.CODE § 24-4.9 et seq.).

208. *Pisciotta*, 499 F.3d at 637 (noting that "[w]e nevertheless find this enactment by the Indiana legislature instructive in our evaluation of the probable approach of the Supreme Court of Indiana to the allegations in the present case.").

209. *Id*. at 637 (emphasis added).

210. *Id*. While lacking access to the plaintiffs brief in this case, it may be the plaintiffs reached this conclusion on the fact that it is a violation of the same statute to dispose of PII in a public area if the information has no encryption or other protection. Dump the hard copy data in a dumpster, and at that moment, you have committed a violation of Indiana law.

211. *Id*. at 635.

212. *Id.* at 635.

two potential harms or injuries as the court noted, are "coupled" but distinct.

The plaintiff's theory was that "analogous areas" of Indiana law held that plaintiffs had indeed suffered an injury at the moment of data transfer and were entitled to damages as a result.[213] The *Pisciotta* court, as noted, defined this moment as "identity information exposure."[214] Plaintiff offered case law where the court ruled that unauthorized transfer of information was an "actual injury."[215] However, the court differentiated these cases offered by noting that:

> Whatever these cases say about the relationship of banks and customers in Indiana, they are of marginal assistance to us in determining whether the present plaintiffs are entitled to the remedy they seek as a matter of Indiana law. The reputational injuries suffered by the plaintiffs in *American Fletcher* and *Indiana National Bank* were *direct and immediate*; the plaintiffs sought to be compensated for that harm, rather than to be reimbursed for their efforts to guard against some future, anticipated harm. We therefore do not believe that the factual circumstances of the cases relied on by the plaintiffs are sufficiently analogous to the circumstances that we confront in the present case to instruct us on the probable course that the Supreme Court of Indiana would take if faced with the present question.[216]

The language from the court appears to be a rejection of the challenge the court set up for itself. The court noted two distinct elements: one occurring directly and immediately, the "exposure" moment; and, one occurring, if at all, in the "future."[217] However, note in the quote above the court's contention that the plaintiffs harmed in the *American Fletcher* and *Indian National Bank* cases suffered damage that was "direct and immediate." Was not the "information exposure" which the plaintiff's in *Pisciotta* complained of "direct and immediate?"

Yet the court, which initially acknowledged that its challenge was to address two distinct elements, coupled together, jettisoned a major contention of the plaintiffs by concluding that plaintiffs only sought reimbursement for their efforts to prevent future harm. That was, as the court noted, only one part of the plaintiff's theory of recovery. They also sought recovery for "direct and immediate" damage at the moment of transfer and the court simply side-stepped this argument in their opinion.[218] Finally, the court noted that:

> Although not raised by the parties, we separately note that in the somewhat analogous context of toxic tort liability, the Supreme Court of In-

213. *Id.* at 637.
214. *Piscotta*, 499 F.3d at 635.
215. *Id.* at 637-38.
216. *Id*. at 638 (emphasis added).
217. *Id.*
218. *Id.*

> diana has suggested that compensable damage requires more than an exposure to a future potential harm. Specifically, in Allied Signal, Inc. v. Ott, 785 N.E.2d 1068 (Ind. 2003), the Supreme Court of Indiana held that no cause of action accrues, despite incremental physical changes following asbestos exposure, until a plaintiff reasonably could have been diagnosed with an actual exposure-related illness or disease. *Id*. at 1075. In its decision that no compensable injury occurs at the time of exposure, the court relied on precedent from both state and federal courts in general agreement with the principle that exposure alone does not give rise to a legally cognizable injury.[219]

The court faced a conundrum. Being that it was a federal court having to interpret Indiana law, for procedural reasons it was "loath" to approve and impose "novel theories" of recovery on to Indiana.[220] The court noted that "courts are encouraged to dismiss actions based on novel state law claims."[221] When faced with such theories the courts should take ". . .the approach that is restrictive of liability."[222] In the face of this conundrum, the court created a legal fiction that there were no damages occurring from "immediate" injury, the exposure of the information, in order to quell any indeterminism arising from the conflict.

(iii) Criticisms of the Damages Analyses

Not surprisingly, the *Pisciotta* case cited *Stollenwerk* and some of its progeny.[223] The practical effects of *Stollenwerk* and its progeny are clear. It is very difficult to assign liability back to the original holder of the data, the party that suffered the breach. This seemingly neutered liability risk creates disincentives for the holder of the data, the party that profits from possessing the data, from implementing stronger security assurances. More specifically, the reasons for criticizing this holding are as follows:

1. It places all of the responsibility for preventing harm on the shoulders of a party who has no responsibility or capability to ensure the data was secure in the first place, or prevent its acquisition;
2. It puts the responsibly of taking responsive measures on a party most likely unfamiliar with the subtleties, nuances, and dynamics of the misuse of their PII;
3. It does not encourage, or in some cases where the victims do not have the resources to pay for the services in question, discourages, victims to seek professional help in preventing future harm;

219. *Id.* at 639.
220. Piscotta, 499 F.3dat 636.
221. *Id*.
222. *Id.* at 636 (citing Home Valu Inc. v. Pep Boys, 213 F.3d 960, 965 (7th Cir. 2000)).
223. *Pisciotta,* 499 F.3d at 639.

4. It instills an unachievable standard of causation, as courts traditionally define that term in jurisprudence.[224] If expert analysts and investigators within law enforcement, industry and government lament the insufficient data to prove up "reasonable inference[s]"[225] regarding IDC in general, and ID theft in particular, what chance does a citizen-victim on her own have? This is not an argument to dispense with rigorous proof when confronting these issues, nor does it disregard the fact that courts are limited in how liberal and "creative" they can be interpreting the law. However, the practical difficulties in proving causation between data breach cases and subsequent IDC should never be mistaken for the fact that damages directly related to the breach are not occurring; and
5. The court made an artificial and false distinction between the threat to "public health" in the so-called real world versus public health and safety in a digital environment. It is not necessary to precisely equate the two dangers to public health to acknowledge that both are a threat to public health and safety. Citizen-victims, like the plaintiffs in *Stollenwerk* whose data was taken, should not be subjected, by no fault of their own, to something akin to a "reverse lottery"[226] where the unlucky "winners" wait around to be "awarded" their "prize": notification of the manifestation of damages and/or losses as a result of their personal data being stolen.

(iv) Signs of Change, or Merely Outliers?

While pronouncing at the onset that the aim of this article is to raise the level of dialogue about IDC by focusing primarily on the shortcomings of the current decision making in data breach cases, namely the definition and damages elements, this criticism is being born out. Outside of the data breach context, courts have grappled with the issue of whether and when to impose civil liability for identity theft. For example, in a 2003 case, *Huggins v. Citibank,* the Supreme Court of North

224. *See* Bridge v. Phoenix Bond & Indem. Co., 128 S.Ct. 2131, 2142 (2008) (quoting Holmes v. Sec. Investor Prot. Corp., 503 U.S. 258 (1992), that courts "demand for some direct relation between the injury asserted and the injurious conduct alleged."). However, the *Bridge* court also noted in *Holmes* that, "[p]roximate cause, we explained, is a flexible concept that does not lend itself to 'a black-letter rule that will dictate the result in every case.'" *Id*. at 2142 (citing *Holmes*, 503 U.S at 272).

225. *Stollenwerk,* 2005 U.S. Dist. LEXIS 41054 at *17 (stating that "[w]here evidence is circumstantial, it must permit a jury to draw reasonable inferences, not merely speculate or conjecture." (citation omitted)).

226. Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules,* 64 U. PITT. L. REV. 343, 362 (2003) (using "Reverse lottery," Daniel J. Solove's phrase).

Carolina declined "to recognize a legal duty of care between credit card issuers" and identity theft victims, commenting that even though "it is foreseeable that injury may arise by the negligent issuance of a credit card, foreseeability alone does not give rise to a duty."[227] The *Huggins* court held that given the lack of an "existing relationship" between the plaintiff and bank, the bank owed no duty of care to the plaintiff.[228]

However, a recent case with a similar fact pattern resolutely disagreed with the holding in *Huggins*. In *Wolfe v. MBNA*,[229] a federal court held that:

> Upon review, the Court finds the South Carolina Supreme Court's conclusion in *Huggins* to be flawed. In reaching its conclusion, the *Huggins* court relied heavily on the fact that there was no prior business relationship between the parties, that is, the plaintiff was not a customer of the defendant bank. The Court believes that the court's reliance on this fact is misplaced. While the existence of a prior business relationship might have some meaning in the context of a contractual dispute, a prior business relationship has little meaning in the context of negligence law. Instead, to determine whether a duty exists between parties, the Court must examine all relevant circumstances, with emphasis on the foreseeability of the alleged harm. As to the issue of foreseeability, the South Carolina Supreme Court found that "it is foreseeable that injury may arise by the negligent issuance of a credit card" and that such injury "could be prevented if credit card issuers carefully scrutinized credit card applications." The Court agrees with and adopts these Findings.[230]

The *Wolfe* court went on to note that "[w]ith the alarming increase in identity theft in recent years, commercial banks and credit card issuers have become the first, and often last, line of defense in preventing the devastating damage that identity theft inflicts."[231] Finally, In *Bell v. Michigan Council*, the court determined that ID theft resulting from database breach was a foreseeable consequence, and therefore found de-

---

227. Huggins v. Citibank, 585 S.E. 2d 275, 277 (S.C. 2003) (citing S.C. State Ports Auth. v. Booz, Allen, & Hamilton, Inc., 346 S.E. 2d 324, 325 (1986)). *See also* Pointes of Plantation Pointe Owners Ass'n v. Rockwell, No. 2005-UP-579 (S.C. Ct. Apps. Nov. 22, 2005), *available at* http://www.judicial.state.sc.us/opinions/displayUnPubOpinion.cfm?caseNo=2005-UP-597.

228. *Huggins,* 585 S.E. 2d at 277.

229. Wolf v. MBNA Am. Bank, 485 F. Supp. 2d 874, 881-882 (W.D. Tenn. 2007). *See also* Brunson v. Affinity Fed. Credit Union, No. A-4439-06T1, 2008 N.J. Super. LEXIS 193 (N.J. Super. Ct. App. Div. Sept. 9 2008) (holding that fraud investigators have a duty to "pursue with reasonable care their responsibility for protecting not only their own customers, but non-customers who may be victims of identity theft."); Mary Pat Gallagher, *Identity-Theft Victims Owed Duty of Care in Bank Fraud Investigations, N.J. Court Says*, LAW.COM, Sept. 11, 2008, http://www.law.com/jsp/article.jsp?id=1202424426977.

230. *Wolf*, 485 F. Supp. 2d at 882.

231. *Id.*

fendants liable for damages incurred by the plaintiffs resulting from the breach.[232]

As promising as this appears to would-be IDT victims, we must note that this holding goes out on a limb. The *Bell* court hung its hat on a unique circumstance, namely the special relationship between a union organization and its union members.[233] In fact, the court found this relationship had elements of a fiduciary relationship and as such, the defendants were on notice they had to take special steps to protect plaintiff's information.[234] Failing in these steps it was foreseeable that the data could be stolen, and if stolen, subject to ID theft. Since this is exactly what happened in the *Bell* case, the court was satisfied that a causal relationship existed between the loss of the data and the subsequent abuse of the data.

In addition to the non-data breach cases, the most recent cases involving data breaches may be a foreshadowing that the judiciary is moving in the direction of recognizing actual injury the moment the data is transferred. In November 2007, the court in *American Federation of Government Employees v. Hawley* (*TSA*)[235] examined the issue of damages resulting from a theft of a laptop computer that held PII of workers for the Transportation Security Administration.[236] The plaintiffs had alleged that "the defendants violated the Aviation and Transportation Security Act (ATSA), 49 U.S.C. §§ 44901 and 44935, and the Privacy Act, 5 U.S.C. § 552a, by failing to establish appropriate safeguards to insure the security and confidentiality of personnel records."[237]

Defendants sought dismissal on the grounds that the plaintiffs in the case suffered no actual injury as a result of the breach.[238] Defendants claimed, among other defenses, that "individual plaintiffs lack standing because their allegations of harm are speculative and dependent upon third parties' criminal actions," and therefore failed to "demonstrate an injury-in-fact."[239] The court rejected this argument noting that "in this circuit, 'emotional trauma alone is sufficient to qual-

232. Bell v. Mich. Council 25, No. 246684, 2005 Mich. App. LEXIS 353 (Mich. Ct. App. Feb. 15, 2005).

233. *Id.* at *5.

234. *Id.* at *9-10.

235. Fed'n of Gov't Employees, 543 F. Supp. 2d 44 (D.C. Cir. 2008).

236. *Id*. at 53. Plaintiffs alleged that the defendants "violated the Aviation and Transportation Security Act ("ATSA"), 49 U.S.C. §§ 44901 and 44935, and the Privacy Act, 5 U.S.C. § 552a, by failing to establish appropriate safeguards to insure the security and confidentiality of personnel records." *Id*. at 45.

237. *Id.*

238. *Id.* at 50-51.

239. *Id.* at 50.

ify as an 'adverse effect',[240] and therefore not dependent on the actions of 'criminal third parties.'"[241]

Further, in *Ruiz v. Gap, Inc.,* decided in March of 2008, the court held that Joel Ruiz was entitled to move forward with his complaint against the Gap in a case that started when someone stole a laptop containing Ruiz's personal information.[242] Ruiz claimed he had suffered actual injury resulting from the use of the stolen data. While Ruiz did not claim the thieves stole his identity, he did claim that he was at a heightened risk of ID theft. Defendant claimed this meant he had not suffered actual injury and therefore the court should have dismissed the case. The court rejected that claim, noting that "to confer standing, the threat of future injury must be credible rather than remote or hypothetical."[243] The court concluded, with some cautionary language directed towards the plaintiff, that he had in fact met this threshold.[244]

While both cases are not directly on point to data breach notification cases, they nevertheless indicate reluctance on the part of the courts in question to accept the heretofore nearly unassailable argument that loss, or theft of data, does not equate to an "actual injury." Note however, some courts are demonstrating a different posture when it comes to hot button copyright litigation, where there appears to be a willingness to make an inferential leap between cause and effect by relying on indirect proof.[245]

(b) "No Damages": A Mistaken Social Fiction

In keeping with the contention of this section that damages analyses are fictions created and perpetuated in the wake of data breaches, the second manifestations are social fictions. The failure of the legal system to assess the extent of injury accurately, and therefore possible damages or loss in the wake of data breaches, is only one factor contributing to our inadequate understanding of the nature and scope of the ID theft. In

240. *Id.* at 51 n.12 (citing Krieger v. Dep't of Justice, 529 F. Supp. 2d 29, 53 (D.C. Cir. 2008)).

241. *Id.* at 51 n.12.

242. Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1124 (N.D. Cal. 2008).

243. *Id.* at 1126 (quoting Hartman v. Summers, 120 F.3d 157, 160 (9th Cir. 1997)).

244. *Id.* at 1126 ("[s]hould it become apparent that Ruiz's alleged injury is in fact too speculative or hypothetical, the Court will conclude, as it must, that Ruiz lacks standing.").

245. A similar argument –as to how courts determine recoverable injury– can be found in copyright context. In *Capitol Records Inc. v. Thomas,* the MPAA's argument rested on how one defines distribution in the copyright context. David Kravits, *An Essay Concerning MPAA Understanding of "Making Available" in the P2P Context*, WIRED, June 24, 2008, http://blog.wired.com/27bstroke6/2008/06/an-essay-concer.html. U.S. District Judge Michael Davis instructed jurors they could find unauthorized distribution –copyright infringement– if Thomas was making available the copyrighted works over a peer-to-peer network. *Id.* The jury decided her liability in five minutes. *Id*.

addition to this legal fiction, flawed social fictions arise from the failure of other social institutions to accurately classify and assess the value of PII. Both legal and social fictions are coping mechanisms used to bring determinisms to the information chaos wrought by IDC, and the value of those fictions is measurable by how closely they acknowledge the reality of the harm incurred.

Whereas legal fiction explicitly categorizes whether PII theft qualifies as damages by artificially drawing lines in time and space, social fiction implicitly influences damages analyses by failing to recognize (in verbal discourse) the commoditization of personal information, while at the same time treating it in practice like other goods in the marketplace. The result is that institutional and social protections and conventions that would normally attach to goods (like financial standards for asset valuation) do not attach to personal information, thus ultimately leaving a policy gap against which damages are otherwise measured.

What is causing society to react to identity data theft is a perception, institutionalized within our control processes and cultural conventions, which is slow to grasp that personal and transactional data is no longer external to that which we have structured our commerce around in a tangible sense. Rather, it has become a highly valuable commodity in and of itself.[246] A familiar adage of our IT society, "the message is the medium"[247] has evolved into "the product is the person."[248] Although current social fiction resists explicitly labeling PII as a tradable commodity, nonetheless, this notion will assimilate and internalize along the same trajectory of other social norms as the public continues its exposure to news stories and firsthand accounts of the maturation of the white, grey and black markets in PII, including those related to ecommerce and breeder identification.[249] Somewhere along that continuum, the public

246. *See* Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services,* 39 SAN DIEGO L. REV. 943, 953 (2002) ("Indeed, the former chairman of Citicorp referred to the information standards for the movement of personal and nonpersonal financial data as the equivalent of money in global financial markets."). For a discussion of the already large market in personal information, including the selling of personal information on markets, see Kenneth C. Laudon, *Markets and Privacy*, COMMUNICATIONS OF THE ACM, Sept. 1996, at 92, *available at* http://www.eecs.harvard.edu/cs199r/readings/laudon.pdf.

247. MARSHALL MCLUHAN, THE MEDIUM IS THE MESSAGE (2005). *See also* Wikipedia, *The Medium is the Message,* http://en.wikipedia.org/wiki/The_medium_is_the_message (as of Apr. 8, 2009, 18:19 GMT).

248. Which is to say that the optimal goal behind online advertising and transactions is to shrink the transaction costs between the buyers and sellers of goods/services, such that if achieved, the customer-buyer is the sum of his transactions and purchased products.

249. Breeder documents are documents that are used to obtain other documents used for identity; e.g., a birth certificate is used to obtain a drivers license which is then used as an identity document. *See, e.g.*, Social Security Administration, Report to Congress on Options for Enhancing the Social Security Card, http://www.ssa.gov/history/reports/ssnreportc4.html (last visited Nov. 9, 2008).

will view the failure to adequately manage PII and transactional data as a failure of the control institutions (legislative, judicial and political) to protect citizens, both individually and in the aggregate.

(i) Evidence Supporting Actual Damages: Wounded Victims

The Federal Trade Commission understood the damages fictions and hurdles that plaintiffs in a DBN action face all too often. This understanding led the FTC to request from Congress a strict liability standard for violations of Section 5, The Unfair and Deceptive Trade Practices Act.[250] The FTC, with its broad investigatory powers and responsibilities, was hesitant to take on the burden of establishing the causal damages standard impelled by the courts on victims of data breaches, but also would not turn a blind eye to real damages suffered by citizen-victims.

The FTC illustrated its discord with the "no damages" legal fiction in its enforcement action against BJ's Wholesale Club, in which the following occurred:[251]

> Beginning in late 2003 and early 2004, banks began discovering fraudulent purchases that were made using counterfeit copies of credit and debit cards the banks had issued to customers. The customers had used their cards at respondent's stores before the fraudulent purchases were made, and personal information respondent obtained from their cards was stored on respondent's computer networks. This same information was contained on counterfeit copies of cards that were used to make several million dollars in fraudulent purchases. In response, banks and their customers cancelled and re-issued thousands of credit and debit cards that had been used at respondent's stores, and customers holding these cards were unable to use their cards to access credit and their own bank accounts.

The FTC settlement agreement laid the liability for the damage in the wake of the breach right on BJ's doorstep.[252] However, nowhere in the settlement agreement does one find claims or admissions that there was a direct causal relationship between the data breach and the ultimate misuse of the data in question.[253] Indeed, a direct causal relation-

250. S*ee* Lisa Jose Fales & Jennifer T. Mallon, *The FTC's Use of its Unfairness Jurisdiction in Data Security Breach Cases: Is it Fair?*, THE SECURE TIMES, Sept. 1, 2006, http://www.thesecuretimes.com/2006/09/the_ftcs_use_of_its_unfairness.php.

251. Complaint for Plaintiff, BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005), *available at* http://www.ftc.gov/os/caselist/0423160/092305comp0423160.pdf. We chose not to include this case in the *Stollenwerk* progeny section because the case settled by consent on June 16, 2005, prior to an opinion issued by the court regarding a motion to dismiss.

252. *See* Press Release, Federal Trade Commission, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), *available at* http://www.ftc.gov/opa/2005/06/bjswholesale.shtm [hereinafter Press Release, BJ's Wholesale].

253. In the Matter of BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005).

ship would be nigh impossible to prove. Given the existence of the black market in data and myriad potential white market sources for any particular piece of stolen data, the task of tracing any instance of fraud *directly, in the legal sense*, back to any particular breach is in many cases futile.[254] In other words, the evidence that a particular data holder is directly liable for a particular instance of fraud is often circumstantial at best.

How exactly would the FTC, or for that matter other government agencies or law enforcement, prove direct causation once the data had been posted online, short of proving who posted the data in the first place? This would essentially amount to trying to prove a negative: that there was no other avenue from which this information could have been stolen and ended up for sale on the black market. However, the FTC recognized that damages are real and present so it forced BJ's into a settlement decree consisting of a hefty fine for damages without proof of causation or acknowledgement of liability.[255] Depending on one's perspective, it either created a new fiction that inferred damages from the mere act of the data being exposed, or it usurped the prevailing fiction ("no damages") by eliminating the causation requirement and deeming the proof of breach enough to hold BJ's responsible for correlative damages.

Anecdotal support for the enduring damages resulting from IDC is provided by a survey conducted by Nationwide Mutual Insurance Company, and reported in many news outlets.[256] The survey found that "28 percent of identity thieves' marks are not able to reconstruct their identities even after more than a year of work."[257] Furthermore, the effort expended to mitigate the damage averaged eighty-one hours per victim.[258] The average total of fraudulent charges was fairly high: $3,968.[259] But only sixteen percent reported that they were held responsible for at least some of the charges.[260] A majority of victims discovered the fraud, not by being notified by their bank, but by noticing unusual charges on their statement.[261] However, it took an average of five and a

254. *See* Kimberly Kiefer Peretti, *Data Breaches: What the Underground World of "Carding" Means*, 25 SANTA CLARA COMPUTER AND HIGH TECH. L. J. (forthcoming).

255. *Id.*

256. A Google search for "nationwide mutual insurance identity theft survey" turns up 31,700 hits (conducted Oct. 28, 2008).

257. See One In Four Identity-Theft Victims Never Fully Recover, INFORMATION WEEK, July 26, 2005, http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=166402700 [hereinafter One in Four].

258. *Id.*

259. *Id.*

260. *Id.*

261. *Id.*

half months from the time of the theft to when it was discovered.[262] "Only seventeen percent were notified by a creditor or financial institution of the suspicious activity, a figure which if accepted, would be the type to fuel federal lawmakers pondering legislation that would require public disclosure of large data breaches."[263]

This information indicates, among many other things, the ongoing battles that consumers and agencies assigned to protect them have with simply identifying and rectifying damages resulting from IDC. These difficulties are inherent to and a remnant of an environment lacking reporting and resolution capabilities. This then feeds the recursion of legal fictions that fail to recognize IDT damages and compensate victims accordingly. Regardless of the fictions rendered by judicial "no-damages" or the failure by policymakers to acknowledge industry's handling of digital identity as a commodity, there is no debating that IDC is costing citizen-victims economically and psychologically.

(ii) Market Hypocrisy

This article offers the actions of the market economy itself as a second counterproof of the prevailing legal fiction behind the courts' failure to recognize actual injury or IDC damages in wrongful identity acquisition scenarios. Specifically, companies and associated goods and services sprouting in the wake of the growth of IDT believe the legal conclusions that there are no damages or loss incurred. We are witnesses to a burgeoning, multimillion dollar industry in identity management proffered to provide solutions to a problem which we do not seem to recognize when it comes to liability or responsibility to prevent. The FDIC Cyber Fraud and Financial Crime Report, which is a centralized collection of information related to cyber fraud and financial crimes that impact financial institutions, for the second quarter of 2007 documented a smattering of statistics that fly in the face of claims that IDT damages are not occurring.[264] For example:

> [t]he number of consumer records breached doubled compared to prior quarters; the number of computer intrusion Suspicious Activity Report ("SAR") filings are relatively low but growing at a fast pace; the estimated mean (average) loss per SAR almost tripled the estimated mean loss per SAR identified one year ago; online bill payment applications

262. *Id.*

263. *One in Four*, *supra* note 257. *See also* Robert Gellman, Privacy, Consumers, & Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete (2002), *available at* http://www.epic.org/reports/dmfprivacy.html.

264. *See* Division of Supervision and Consumer Protection, Cyber Fraud and Financial Crime Report (2007), *available at*http://blog.washingtonpost.com/securityfix/FDIC%20INCIDENT%20REPORTR2Q07r.htm.

> were most frequently targeted by cyber thieves; however, unauthorized access to ACH[265] and wire transfer applications caused the most losses to FIs[266] in the computer intrusion category; ID theft SARs filing increased fifty-nine and four percent during the 2Q06 2Q07, respectively, and ID theft often results from data breaches outside of insured-FIs, but FIs suffer losses when the data is used to commit account application fraud; ID theft and account takeover was the most frequently *identified* type of computer intrusion that occurred during the 2Q07; unknown unauthorized access to online banking has risen from 10 to 63 percent in the past year; and, unauthorized automated clearing house (A CH) and wire transfers caused the most losses to FIs because of faster funds availability, with wire transfer SARs increased 44 percent from 2Q06 and doubled compared to 2Q05.[267]

Cited next is a recognized market leader in identity risk management as an illustration of the contradictory actions and information propagated. Although the next section dissects this dynamic more fully, the conflict of interest exposes itself in the interplay between: (a) the conclusory statistics and probabilistic determinations about the low rate of identity misuse from breaches; and, (b) the coincident advocacy for identity risk management services because of the "growing" threat of identity fraud.[268]

In other words, based on proffered data from some identity theft risk management vendors, citizen-victims of data breaches stand a slight chance that their identities will actually be used when their PII is stolen, yet at the same time corporate-victims are being urged to engage these claimed solution providers to curb fraud from those same breaches.[269] Accepting this as true, risk analytics related to IDT victimization is in-

---

265. Automated Clearing House. *See* NACHA, What is ACH?, http://www.nacha.org/About/what_is_ach_.htm (last visited Nov. 22, 2008).

266. Financial Institutions ("FIs").

267. Press Release, BJ's Wholesale, *supra* note 252.

268. *See e.g.* Press Release, ID Analytics, The Telecommunication Risk Management Association (TRMA) Honors ID Analytics' Mike Cook with the 2006 President's Award (Feb. 14, 2007), *available at* http://www.idanalytics.com/news_and_events/20070214b.html.

269. *See, e.g.*, ID Analytics, Inc., ID Analytics for Data Defense: Maintaining the Trust You've Earned, http://www.idanalytics.com/solutions/datadefense.html (showing an example of an identity theft solution provider's advertisement). Specifically, the advertisement states:

> in the unfortunate event that evidence of data theft is found, the ID Analytics for Data Defense solution provides breach analysis services free of charge. Breach analysis services are used to determine whether a specific breach has resulted in identity theft in order to provide the precise information required to minimize harm and take restorative action. ID Analytics will work with you to identify the source of compromise.

Id. Debix is another example of a company purporting to offer identity theft services. Debix Data Breach Services, http://www.debix.com/business/index.php (last visited Apr. 18, 2009).

creasingly in demand to bring certainty to the legal risk because they can have significant economic benefits for the breached companies. For one, this predictive risk analysis may be useful to establish whether breach notification responsibilities are triggered. If there is not a "reasonable likelihood"[270] that identities have been or will be compromised, for example, the breached company can avoid the costs associated with notification.[271] Even if organizations decide to notify, the rationalization is that the cost of contracting these same services for victims outweighs the negative public relations and reputational costs of not notifying. Second, even if notification is triggered, identity risk analyses can be leveraged to characterize the risk of use to feed the legal fiction regarding damages. In such a case, if one's identity is unlikely to be misused in the future, there are no damages to the citizen-victims and thus no legal liability risk from potential litigation, class action or otherwise.[272]

The picture painted is one of a near victimless crime, yet it is one that spawns costly damage for industry. Crafted in this way, the risk is real enough to justify remedial and preventative services by industry, yet not so threatening to the consumer-victims such that they should retreat from the electronic marketplace. This hypocrisy is further evidenced if one considers some of the holdings of respective courts which deny damages, in light of the following-logic: if identity risk management services are influencing company's credit and loan decisions (i.e., "deny applicant X because she is a bad identity risk"), is that not a "manifestation" of the ID theft that courts are basing their damage determinations on?[273] Further, the corporate-victim is damaged from what is purport-

270. Statutes have used various comparable standards, such as "possible risk", likely risk", etc. *See, e.g.,* CONN. GEN. STAT. § 36a-701b (2008) (effective Jan. 1, 2006) (applying a likelihood of harm standard); WASH. REV. CODE § 19.255.010 (LexisNexis 2008) (effective July 24, 2005) (using a standard of reasonable likelihood of risk of criminal activity); DEL. CODE ANN. tit. 6, § 12B-102 (2008) (effective June 28, 2005) (using a likelihood of misuse standard).

271. For example, costs are incurred from remedial actions such as printing and postage of notification letters, retaining legal services to address the legal issues, offering credit monitoring subscriptions to customers, establishing and implementing a toll-free customer support hotline and contract call center, and the more oblique costs related to customer defections.

272. Besides using quantitative, probabilistic bases for painting the risk the misuse of PII, identity risk analytics can and have used qualitative labeling to support the same end. For example, a popular and prevailing theory is that "synthetic" identity theft is the largest threat. Since this manifestation involves combining identity artifacts from multiple, compromised "real" persons to create a new identity to misuse, such "evidence" can be used to support an argument that the risk of IDT is low, either to subvert notification triggers or litigation damages thresholds.

273. *See* Section II.2(B)2, *supra*, Damages Conundrum: Fictions Created and Perpetuated in the Wake of the Data Breaches.

edly the largest identity fraud threat, synthetic identity fraud.[274] Who bears those costs? Someone must bear the costs of the losses from synthetic fraud in excess of fifty dollars. These costs must get passed along to citizen-consumers in the form of nebulous and opaque increased fees and premiums, like in the physical world shoplifting situations. Again, reality belies the social fictions that do not acknowledge the damages.

Even if one were to accept the claim that these costs are miniscule, unlike shoplifting, electronic "identity lifting" affects, as we previously noted, the citizen beyond just increased prices –it carries the risk and costs of missed opportunities and heightened pricing for loans, insurance, credit card rates, as well as the outright denial of these economic enablers. Admittedly, just as the difficulty in connecting the breach with the illegal use to justify denial of damages, so too will the difficulty in proving missed and increased opportunity costs be used to deny the claims plaintiffs put forward.

Another market dynamic which reveals the social fiction that there are no, or few, legally recognizable damages from IDT, is the actions of breached companies, what has become a de facto response in the wake of breaches. Specifically, separate from any legal liability determinations, individuals whose names are exposed in breaches are often provided one year's worth of free credit monitoring and their exposed credit cards are cancelled and new cards issued.[275] These gestures are couched as "precautionary" measures by the breached company and are served up on a platter of customer good will. Some companies even go so far as to assure customer-victims that they will get the data back and prevent its future use.[276] While these gestures are a first line response to assuring customers that that they will bear no costs, is labeling these responses as "remedial" rather than "proactive" an attempt to avoid admitting that damages have resulted?

---

274. "Synthetic fraud is quickly becoming the more common type of identity fraud, surpassing "true-name" identity fraud, which corresponds to actual consumers. In 2005, ID Analytics reported that synthetic identity fraud accounted for 74 percent of the total dollars lost by U.S. businesses to ID fraud and 88 percent of all identity fraud 'events' –for example, new account openings and address changes." Leslie McFadden, *Detecting Synthetic Identity Fraud*, May 16, 2007, http://www.bankrate.com/brm/news/pf/identity_theft_20070516_a1.asp.

275. *See, e.g.*, Ross Kerber, *Banks Claim Credit Card Breach Affected 94 Million Accounts,* INT'L HERALD TRIBUNE, Oct. 24, 2007, http://www.iht.com/articles/2007/10/24/business/hack.php; David M. Ewalt, *Are Companies Liable for ID Data Theft?*, FORBES, Apr. 14, 2005, http://www.iht.com/articles/2007/10/24/business/hack.php.

276. For example, "In March 2005, the parent company of Lexis Nexis said hackers got access to personal information of as many as 32,000 U.S. citizens in a database owned by Lexis Nexis. . .." Melissa Campanelli, *Certegy "Doing Everything Possible" to Ensure Trust With Consumers After Data Breach,* DMNEWS, July 5, 2007, http://www.dmnews.com/Certegy-quotdoing-everything-possiblequot-to-ensure-trust-with-consumers-after-data-breach/article/96133/.

Or, regardless of the labeling, does the fact that companies take these measures prove that the likelihood of damages to individuals is real? One does not have to wait for a court to determine whether damage have "manifest" themselves to know that someone is paying for the credit monitoring and card reissuance of millions of individuals. Again, although IDC numbers are shrouded, one can infer that the magnitude of losses have reached a tipping point for credit card companies by virtue of the recent implementation of a strict liability standard on breached merchants.[277] Merchants seem to have gotten the message. On October 4, 2008 the National Retail Federation, the trade organization representing many of the retailers in the nation, issued a press release requesting that major players in the credit card industry drop, or at least alter, its requirements that the merchant hang on to point of sale data:

> "All of us—merchants, banks, credit card companies and our customers—want to eliminate credit card fraud," said NRF Chief Information Officer David Hogan in the letter. "But if the goal is to make credit card data less vulnerable, the ultimate solution is to stop requiring merchants to store card data in the first place."[278]

(iii) Public Policy

The third basis for refuting the current "no damages" fictions is grounded in the policy that our public health demands that IDC solutions be dealt with at some level from a social-good perspective rather than from a compartmentalized, market-centric one. The risk of treating IDC as a self-correcting problem for the market to solve is that tangible and latent costs and responsibility for identity fraud will continue to be dispersed and externalized to the point where we will have polluted the reliability of the information which is fueling our society. In other words, there is a public health reason to prevent information chaos and corruption.[279]

---

277. Minnesota has recently passed a law that, using a strict liability standard, makes merchants liable to card issuers for costs incurred by the issuers as a result of a breach of the merchants' database. MINN. STAT. § 325E.64 (2007).

278. *See* National Retail Federation, *NFR to Credit Card Companies: Stop Forcing Retailers to Store Credit Card Information*, Oct. 4, 2007, http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=380.

279. To be sure, there are counterarguments that restricting the market's use of PII is bad for public policy. One position holds that there has been no demonstrated harm of utilizing PII for behavioral targeting or third-party advertising. Further, some claim that regulating the Internet along these lines threatens the openness and free services and content– a major business model supporting the Internet. Also, some believe that norms and expectations have already been established such that people have been assimilated to the online buying and selling of PII by ad companies. One major point is echoed by New York Assemblyman Richard L. Brodsky: "In the end, I don't have a philosophical objection to targeting, if it's done with permission, but it is absolutely clear that people right now do not understand what they're actually giving up." Louise Story, *A Push to Limit the Tracking of*

True to the nature of a market-dominated economy, as long as profits from the former outweigh costs from the latter, rational businesses will not have incentives to choose the safeguard route. Under this market-centric framework, until the cost of preventing IDC by instituting safeguards and shouldering liability for data breaches surpasses the cost of losses due to IDC, there is no financial incentive for business to alter their strategies and practices. The problem with this incentive framework, relying as it does on market self-correction, is that it presumes to account for all the costs of IDC. Besides the fact that lack of reliable IDC data prevents the financial costs of IDT from exposure to consumers and regulators, direct financial losses are only part of the picture.

The indirect and social costs of IDC go beyond the strictures of a balance sheet view of the world. The injuries to individuals have been well documented.[280] Apart from psychological harms, there are the missed opportunity costs and downstream effects from denial of loans and credit, and increased premiums.[281] Absence of standards to measure the indirect-financial losses of IDT does not mean they do not exist. Making the citizen-victim financially whole is only one part of the solution. Breach notification thresholds based on manifestation is shortsighted. Downstream, latent identity integrity damage renders the current protection regime something other than the zero-sum game that financial institutions advocate when they claim that citizen-victims are not out of pocket for fraudulent transactions committed by a third party.[282] We have yet to realize the consequences of making the corrup-

---

Web Surfers' Clicks, N.Y. TIMES, Mar. 20, 2008, *available at* http://www.nytimes.com/2008/03/20/business/media/20adco.html?fta=y

280. "In fact, such non-monetary harm, although difficult to quantify, may cause more damage to identity theft victims than quantifiable monetary loss." Haeji Hong, *Dismantling The Private Enforcement Of The Privacy Act Of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 108 (2005) (describing the significant non-monetary harm cause by IDT: lost time, emotional distress, incidental financial problems, law suits, arrests, etc.). These harms of IDC are similar to what is described more fully in the context of the dangers of market solutions in next section 3(a) Handicapping Horses.

281. *See* NEWMAN, *supra* note 42. Newman and McNally point out that societal costs include, among other things:

> public safety risks/threats; burdens created by the presence of illegal immigrants; potential constitutional intrusions underlying proposed schemes for a national centralized information database, national ID cards, or the use of biometric methods of identification - and their associated financial costs; higher premiums or other costs passed on by companies to consumers; increased paranoia, which may also result in financial costs associated with the purchase of preventive insurance or other methods of personal identity theft prevention; and overall decreased confidence in the promised benefits of the information age.).

Id.

282. "Visa issued a statement saying it knows of the data security breach and is working with authorities and banks to monitor and prevent fraud. As with MasterCard and Discover, Visa noted that card users are not responsible for fraudulent transactions." Joris

tion of identity integrity a negative externality of market control. What are the implications of a free market approach to protecting constitutional rights (i.e., privacy, identity integrity) which is predicated on an individual consumer's ability to negotiate and demand more identity protection? Should not individual identity be an inalienable right that cannot be commoditized?

For example, just because we have not fashioned a way to put numbers to the cost of having one's SSN stolen and used indeterminately in time or place, or cannot quantify the harms from having one's transactions dossier'd by state-sponsored or criminal enterprise, or behavioral marketing intelligence efforts, does not mean that no damages will or have occurred. Further, by allowing instant credit policy to drive the train, while more turnstiles for credit are opened for citizen-consumers they also allow entry for opportunistic and targeted identity thieves.[283]

One of the most obvious showings of information corruption and prescience of a chaotic environment is found in the pervasive growth of spam and phishing –identity theft of the corporate variety and simultaneously a vector to the personal variety. The exponential growth of these attack vectors not only clogs bandwidth and expends the attention of

---

Evers, *Credit Card Breach Exposes 40 Million Accounts*, CNET NEWS, June 18, 2005, http://news.cnet.com/Credit-card-breach-exposes-40-million-accounts/2100-1029_3-5751886.html. *See also* OECD, SCOPING PAPER ON ONLINE ID THEFT, *available at* http://www.oecd.org/dataoecd/35/24/40644196.pdf. The report states:

> In testimony before the Ohio state legislature, the US FTC explained how the loss is allocated between individuals and businesses, stating that: [US] [federal law limits consumers' liability for unauthorized credit card charges to USD 50 per card as long as the credit card company is notified within 60 days of the unauthorized charge. See 12 C.F.R. § 226.12(b). Many credit card companies do not require consumers to pay the USD 50 and will not hold the consumers liable for unauthorized charges, no matter how much time has elapsed since the discovery of the loss or theft of the card. Consumers' liability for unauthorized debit card charges is limited to USD 50 in cases where the loss is reported within two business days, and to USD 500 if reported thereafter. See 15 U.S.C. § 1693g (a). In addition, if consumers do not report unauthorized use when they see it on their bank statement within 60 days of receiving the notice, they may be subject to unlimited liability for losses that occurred after that period. *ID Public Entities, Personal Information, and Identity Theft, Hearing Before the Ohio Privacy and Public Records Access Study Comm. of the Ohio Senate and House of Representatives* (2007) (statement of the US FTC, delivered by Betsy Broder, Assistant Director of the Division of Privacy and Identity Protection).

Id. at 62.

283. This 'instant credit mentality' can be seen on display in the subprime debacle. Easy credit and lax background checks were a bonanza for ID fraud specialists. The fraudsters now face new challenges now however, as access to credit tightens up. *See* Bob Tedischi, *Thieves Tap Into Home Equity*, N.Y. TIMES, July 27, 2008, *available at* http://www.nytimes.com/2008/07/27/realestate/27mort.html?_r=1&scp=1&sq=theives%20tap%20equity&st=cse&oref=slogin ("Now that lenders have vastly tightened their lending criteria, criminals who specialize in mortgage fraud have little choice but to move upstream and seek out victims with good credit.").

human and systems processing, but it concurrently pollutes the credibility of corporate and individual digital identities.[284] While the arms race between security controls and hackers assures us that attack vectors will be exposed and closed, the ability to measure and remediate damage to corporate reputation and information validity among readers and visitors' is way beyond the capacity of technical engineering repair.

Instances of end users fooled and defrauded by email schemes are notorious and legion.[285] Undoubtedly, business strategies designed solely or primarily around email communications (targeted marketing, business development, brand building) with citizen-consumers have been altered or rendered futile. PayPal, eBay and the Internal Revenue Service are consummate poster children for the budding chaotic digital environment as a result of identity corruption of the corporate rather than individual variety.[286] Stated differently, arguably there is a presumption of illegitimacy attached to email messages received from these organizations.

The justifiable, emerging, apprehension of conducting business electronically shows no sign of retreat. The proliferation of botnets is the most recent and vexing source of information chaos.[287] While estimates vary as to how many hundreds of thousands of computers are unwittingly under the control of criminals, nonetheless their proliferation

284. *See* Secure Computing, Why Corporations Need to Worry About Phishing, Sept. 2004, http://www.ciphertrust.com/resources/articles/articles/phishing.php; Jeff Vance, *Phishing More than a Consumer's Problem*, CIO UPDATE, June 7, 2005, http://www.cioupdate.com/trends/article.php/3510826/Phishing-More-than-a-Consumers-Problem.htm; Michel J.G. van Eeten & Johannes M. Bauer, *Economics of Malware: Security Decisions, Incentives and Externalities*, (2008), *available at* www.oecd.org/sti/working-papers; CLAY WILSON, CONGRESSIONAL RESEARCH SERVICE, BOTNETS, CYBERCRIME, AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS, (2008), *available at* http://www.fas.org/sgp/crs/terror/RL32114.pdf; AARON EMIGH, ONLINE IDENTITY THEFT: PHISHING TECHNOLOGY, CHOKEPOINTS AND COUNTERMEASURES, (2005), *available at* http://www.antiphishing.org/Phishing-dhs-report.pdf.

285. *See supra* note 284. *See* Robert McMillan, *Men Fall Harder Than Women for Internet Fraud, Study Finds,* Apr. 3, 2008, http://www.networkworld.com/news/2008/040308-men-fall-harder-than-women.html?fsrc=rss-security.

286. *See* Juan Carlos Perez, *eBay: Phishing Likely to Blame For Members' Data Theft*, INFOWORLD, Sept. 27, 2007, http://www.infoworld.com/article/07/09/27/eBay-says-phishing-likely-to-blame-for-members-data-theft_1.html; Joris Evers, *Paypal Fixes Phishing Hole*, CNET NEWS, June 16, 2006, http://news.cnet.com/PayPal-fixes-phishing-hole/2100-7349_3-6084974.html; Robert Lemos, *IRS Taxed By Phishing Attacks*, SECURITYFOCUS, Feb. 20, 2008, http://www.securityfocus.com/brief/684.

287. In 2007, technology pioneer Vint Cerf estimated that as many as 150 million machines are infected by bots. Nate Anderson, *Vint Cerf: One Quarter of All Computers Part of a Botnet,* ARS TECHNICA, Jan. 25, 2007, http://arstechnica.com/news.ars/post/20070125-8707.html. *See also* Shadowserver.org, Bot Counts, http://www.shadowserver.org/wiki/pmwiki.php?n=Stats.BotCounts (last visited Aug. 25, 2008).

casts doubt on who is behind a given digital communication.[288] Botnetted end users' systems allow interlopers to masquerade as the legitimate user behind the keyboard, and simultaneously expose any identity artifacts that reside on that system, thus strengthening the ability to impersonate the real person or company.[289]

There are strong public policy arguments that legislative, judicial or free market fictions do not adequately address the real damages stemming from a corrupted information environment. None of these institutional controls has sufficiently accounted for the longitudinal harm to the individual or the aggregate of society.

Coupled with, and compounded by, unreliable and incomplete statistics on IDC, courts reach questionable analytical conclusions with significant consequences. This process, repeated often enough, gains traction as a legal fiction embraced by the courts as well as the holders of PII data. This is a detrimental legal fiction, and injury should be presumed when the data is breached, i.e., the time of exposure.[290] This advocacy should not be mistaken for encouraging and empowering individuals to take steps, as imperfect as those may be at present time, to ameliorate future harm. The presumption advocated in this article incentivizes the entities which posses the data and who are in the best position to protect it, to institute reasonable and appropriate measures to protect society and to spread the cost of heightened protection across a wide spectrum of society.

This presumption also acknowledges what the legal fiction ignores: the core elements of IDC (unauthorized acquisition and use of PII) ex-

---

288. *See* Bruce Schneier: *How Bot Those Nets?*, Wired, *available at*, http://www.wired.com/politics/security/commentary/securitymatters/2006/07/71471. Describing the spread of bots:

> [M]ost bots constantly search for other computers that can be infected and added to the bot network. (A 1.5 million-node bot network was discovered in the Netherlands last year. The command-and-control system was dismantled, but some of the bots are still active, infecting other computers and adding them to this defunct network.)

Id.

289. *See* Bacher et al., *Know Your Enemy: Tracking Botnets*, Aug. 10, 2008, http://www.honeynet.org/papers/bots/.

290. This classification is extrapolated from specific facts of the seminal negligence case dealing with IDT and data breaches, *Stollenwerk v. Tri-West Health Care Alliance*, No. CIV 03-0185-PHX-SRB, 2005 U.S. Dist. LEXIS 41054 (D. Ariz. 2005). The determinative damages question centers around when the breach-related "injury" "occurs" for purposes of the relevant law. At least three possible time pegs are relevant: (1) the time of exposure: when the ID artifacts were vulnerable to breach by thieves during a security incident; (2) the time of detection: when the compromised ID artifacts reasonably could have been diagnosed; and, (3) the time of manifestation: when the breached ID artifacts were "discovered" to have been compromised. *See supra,* II.B.2.b.ii, Stollenwerk Progeny and Analogous Law for discussion of asbestos injury-related triggers for liability.

pand to fit the parameters of their new playing field, the digital Internetworked environment. In the offline realm, misappropriation and abuse of identity is largely fixed, attributable, directly perceived, and bounded (in time and geography); whereas these same actions played out in the online realm are largely experiential, highly mediated, distributed, persistent, anonymous, representational and boundary less, the consequence of which is a very different identity theft threat model. In turn, IDC laws interpreted in the context of the offline realm fail to accommodate for the differing conditions of the online. When the identity data acquisition and use is digital, there are quantitative and qualitative differences in damages and harm to the person behind the identity. In short, a different victimization structure demands a different response and remediation approach.

The public policy argument should curry favor in light of the backdrop of previously described treatment of IDT damages: combine the judicial hesitancy and legal fiction, with forthcoming federal legislation that will preempt the more consumer-protective state laws and will usher in a self-certifying "significant risk" standard for triggering notification mandates. We are arguably on the cusp of the biggest step backwards in privacy protection in decades.

(iv) The Underground Economy: A Black Market in Stolen Identity Artifacts

Finally, there is ample evidence and acknowledgement of a criminal black market in stolen identity information as proof that damages to citizen-victims from IDT are real and consequential.[291] A recent Internet Security Threat Report by cyber protection market leader Symantec attests that the criminals are exchanging stolen full identities for between $14 and $18 and single credit card numbers going for $1 to $6 in this underground economy.[292] This includes a victim's SSN, bank account

291. Peretti, *supra* note 254, stating:

> Large scale data breaches would be of no more concern than small scale identity thefts if criminals were unable to quickly and widely distribute the stolen information for subsequent fraudulent use (assuming, of course, that the breach would be quickly detected). Such wide-scale global distribution of stolen information has been made possible for criminals with the advent of criminal websites, known as "carding forums," dedicated to the sale of stolen personal and financial information. These websites allow criminals to quickly sell the fruits of their ill-gotten gains to thousands of eager fraudsters worldwide, thereby creating a black market for stolen personal information.

292. *See* SYMANTEC INTERNET SECURITY THREAT REPORT: TRENDS FOR JANUARY – JUNE 2007 (2007), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf. The report states:

> Underground economy servers are used by criminals and criminal organizations to sell stolen information typically for subsequent use in identity theft. This data can include government-issued identification numbers, credit cards, bank cards, per-

details including passwords, and other personal information such as date of birth and the victim's mother's maiden name.[293] This report goes further states that the main victims of online identity theft are U.S. citizens, with U.S. based banks issuing eighty-six percent of the credit and debit cards advertised for sale on the online underground. In addition, the United States also played host to fifty-one percent of servers known to host "underground economy" transactions. Symantec could not provide exact figures for the money changing hands in the underground economy, but it estimated it in the hundreds of millions of dollars.[294]

This market has grown so robust and brazen that the criminal "merchants" operating it have taken to publicly posting whether pilfered and proffered credit card accounts are active and viable. This is not just a game of hacker chest beating, but rather, an exhibition of a market that operates on the same principles as aboveground trade in goods and services, where buyers and sellers can reliably valuate the traded commodity.[295] Furthermore, proposed solutions to combating the criminal economy offer an indirect existence proof of what we conjecture to result from this free flow of identities –information chaos. Specifically, some advocate that one of the only viable ways to disrupt the criminal black market is to pollute the reliability of identities and poison the trust of both the criminals' and victims' reputations so as to destabilize the underlying valuation of the identity commodity.[296]

(c) Victimization Risk: Identity Precogs

Flanking attribution and damages analyses, victimization is the last discussed risk analysis resulting from inferences of dubious data and contributing to misinformed policy. Popular advice hailing from some risk analyses quarters is "the more stolen, the less disclosed."[297] For ex-

---

sonal identification numbers (PINs), user accounts, and email address lists. The emergence of underground economy servers as the *de facto* trading place for illicit information is indicative of the increased professionalization and commercialization of malicious activities over the past several years.

Id.

293. *Id.*

294. *See* Kelly O'Connell, *Cyber-Crime Hits $100 Billion in 2007, Out-earning Illegal Drug Trade*, Oct. 17, 2007, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1882

295. *See* Brian Krebs, *Web Fraud 2.0 Fake YouTube Page Maker Helps Spread Malware*, WASH. POST, Sept. 12, 2008, http://voices.washingtonpost.com/securityfix/2008/09/fake_youtube_page_maker_helps.html. *See also* Peretti, *supra* note 254.

296. *See* Jason Franklin, Vern Paxson, Adrian Perrig, & Stefan Savage, *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*, (2007), *available at* http://www.icir.org/vern/papers/miscreant-wealth.ccs07.pdf.

297. For example, IT security breaches are not behind most ID theft. Sarah Hilley, *New Instant Phishing Pop-up Kits on the Rampage*, COMPUTER FRAUD & SECURITY, August 2007, at 10. The US Government Accountability Office (GAO) has said there is limited evidence

ample, recent data from interested stakeholders indicates that there is less chance of being victimized if one's identity is part of large database breach.[298] With regard to data breach threats to IDT, this victimization risk analysis may lead someone to conclude, depending on the precise language of the numerous notification statutes, that there is less legal obligation to notify individuals who data has been compromised. That is because in many of the DBN statutes, as we noted above, the standard for triggering notification is potential harm to the individuals whose data has been breached.

The relevant legal question to tackle in this kind of analysis is: what is the standard for determining "potential harm?" The spectrum of standards ranges from "reasonably possible," to "likely," to "substantial" risk.[299] Notwithstanding the veracity of the supporting evidence, analytical theories that the likelihood of becoming an IDT victim is lower with the larger the number of breached records lend support to decisions notification and related costs are not necessary.

Another theory proffered for reduced notification responsibility in the wake of a large breach is that more notifications just desensitize victims to the potential risk of identity breaches without raising awareness and effective response.[300] The problems with these postures are: (1) they are based on questionable threat model assumptions regarding monetizing and liquidating of identity artifacts; and, (2) they assume a static vulnerability model which ignores the victim's ability to invoke controls such as credit freezes or other monitoring tools to preempt or mitigate illegal use of compromised identities.

As mentioned above, ID Analytics' white paper on national data breaches has described a formulaic rationale to back its assertions that the larger the breach, the less likely the personal data will be misused.[301] This rationale maintains:

---

to suggest that most security breaches lead to identity theft. *See* ID Analytics, Inc., National Data Breach Analysis (2007), http://www.idanalytics.com/assets/pdf/national-data-breach-analysis-overview.pdf [hereinafter *Data Breach Analysis*].

298. *See Experts: Small Risk of Identity Theft in Ohio's Stolen Computer Tape Case*, INSURANCE JOURNAL, June 27, 2007, http://www.insurancejournal.com/news/midwest/2007/06/27/81136.htm ("The smaller the data set, the greater the chances that individuals will be victims of identity theft, the company found.").

299. *Supra* section II.B.i.a.2. The trigger standards for notification vary across states. In general, they break down along some combination of "use risk" and corresponding "outcome." Use risk includes: reasonably-possible, reasonably-believed, risk, reasonably-likely, likely, material risk, substantial risk, significant risk, substantial risk; and outcome includes: breach, misuse, criminal activity, illegal use; harm, loss/injury, economic loss, ID theft/fraud.

300. *See* PERSONAL INFORMATION, *supra* note 47, at 31.

301. *Data Breach Analysis*, *supra* note 297.

> [A]ccepting that it takes approximately five minutes to fill out a credit application, at this rate it would take a fraudster working full-time – averaging 6.5 hours a day, five days a week, 50 weeks a year—over 50 years to fully utilize a breached file consisting of one million consumer identities. If the criminal outsourced the work at a rate of ten dollars an hour in an effort to use a breached file of the same size in one year, it would cost that criminal about $830,000.[302]

We challenge the reliability of these types of assumptions and conclusions by slicing the "fundamental truth" along a different speculative plane.

What if our enterprise product is cigars rather than identities, and owner Joe Smith is a merchant owner who has two employees? Staying true to the "logic" from the analysis above, Joe is unable to recruit more employees to sell his wares, thus limiting cigar sales to that which Joe and his two clerks can transact from their store. Now, suddenly Joe inherits a windfall from the death of his uncle, leader of a national stogie cartel. Similar to the unchallenged assumptions that identity fraudsters are ceilinged-off from processing a large number of "person products," Joe and his crew of two likewise are limited in their ability to sell the large booty and they subsequently pine away in a warehouse humidor.

Arguably, any lucid merchant in Joe's situation would resolve the ostensible dilemma by selling the cigars in bulk to someone else in the cigar business, or for that matter in the business of making money. To be sure, Joe would not extract profit from every cigar, since his offloading would necessitate selling them at a reduced price, i.e., wholesale rather than retail. Recall, however, since Joe paid nothing for the cigars in the first place even the reduced price amounts to a bankroll for Joe. Query why the solution proposed here for Joe's cigars is fundamentally different than what a person engaged in fraud, attaining a windfall of identities faces? Assuming both are incentivized by a virtually guaranteed profit, why would not the purveyors of identities sell the data in the black market economy? The answer is tied to another assumption-turned-social fiction which is spread by victimization risk analyses: the victimization risk from IDT is being calculated *sans* a big, black elephant in the middle of the room: the underground market in PII.[303]

---

302. *Id.* ID Analytics carefully peppers its reports with implicit disclaimers about limitations of its analyses, accompanied by the explicit claims that it is the "ONLY research available today that has looked at ACTUAL breaches. . ." *Id.*

303. ID Analytics, National Data Breach Analysis, *The Data Breach Harm Analysis*, http://www.idanalytics.com/whitepapers/ (last visited Sept. 18, 2008). ID Analytics does attach a disclaimer to its analysis, namely, "The misuse rate could increase drastically if the current for "identities" remains unimpeded and becomes more centralized and efficient." *Id.* To which we ask, how is that we haven't already reached that point, and if we have not, how and who might satisfactorily gauge when that tipping point has occurred. . . it is after all, a market unregulated by the SEC or as transparent as NASDAQ.

Despite the legal fiction encompassed by the courts' failure to recognize IDC damages in wrongful identity acquisition scenarios, the public pressure to address IDC has become apparent amidst a growing demand for control and preventive intervention. If we picture our political economy as an organism as a petri dish, where the ratio of free flowing data substrate to secure PII substrate weighs supreme, a reaction is being catalyzed by the lack of widespread understanding of IDC combined with the deluge of voices clamoring for a solution. One product of this reaction is "identity scoring" or "identity analytics," trade names for IDT victimization risk analysis. Stated differently, identity scoring is a recent market response to the consumer demand for identity control, security, and determinism. ID scoring is the use of risk analytics in a predictive way to engage in identity risk management. For example, identity proofing is the use of identity artifacts (transactional information from various proprietary, public, and private databases) to authenticate an identity based on the statistical probability it is bona fide or has be pilfered.[304]

The harmful significance of identity scoring lies not so much in what the information is, but more so with when and how the information is used. Identity scoring occurs prior to knowledge of any wrongful act or verification of specific reasonable suspicion of criminal activity, to prevent or monitor *possible* IDC activity. This process is different than previous credit risk scoring analytics gathered after specific reasonable suspicion or factual proof of adverse activity has been established.[305] Companies are increasingly turning to ID scoring to engage in the "precogging" of IDC.[306]

---

304. Note the distinction between scoring and proofing. Scoring is a process for measuring the reliability/legitimacy of an identity by matching it with a broad range of available information, and with predicted patterns of behavior. Proofing, on the other hand, is the process of matching a human to a particular token of identity. In other words, making sure someone is who he says he is. Proofing is the complement of authentication. Authentication is the verification of some identity credential or mechanism, like a password or a smartcard. Proofing matches the person to the authentication mechanism. So authentication verifies the identity token. Proofing matches a person to that token. Scoring measures the reliability of such a match. *See* Harold Kraft, *Identity Scoring: New Defense Against Data Breaches,* E-COMMERCE TIMES, Feb. 15, 2007, *available at* http://www.technewsworld.com/story/55770.html?welcome=1205363504&welcome=1205364435&wlc=1220385122; Wikipedia, *Identity Score,* http://en.wikipedia.org/wiki/Identity_score (as of Dec. 16, 2008, 16:53 GMT); *What is Online Identity Proofing and How Does it Work,* Security IT HUB, http://www.security.ithub.com/article/What+Is+Online+Identity+Proofing+and+How+Does+it+Work/212750_1.aspx (last visited Sept. 18, 2008).

305. *See Use and Management of Criminal History Record Information: A Comprehensive Report*, U.S. Department of Justice Bureau of Justice Statistics, http://www.ojp.usdoj.gov/bjs/abstract/umchri01.htm (last visited Sept. 8, 2008).

306. From a business perspective, this is because credit-based exchanges are predicated on knowing an individual's credit/transaction history, which in turn is dependent on being able to correlate the consumer to the record of the consumer's actions. Absent reliable

What is the harm in applying predictive analytic techniques to assess victimization from IDC? The consequences of ID scoring are tenuous given that companies have little incentive to disclose when their use of identity scoring causes harm to their corporation (lost potential customers and profit) or an affected individual (the person whose identity was deemed inauthentic and thus refused goods/services). The underlying techniques are often ill-fitted to the probabilistic conclusions about victimization. The technique has not been deployed long or widely enough for true ID fraud to manifest, and be identified, and such an undertaking is beleaguered by the difficulties of proving a negative. Nevertheless, we might gauge the risks of these identity analytics by comparatively analyzing ID scoring to the pursuit of predicting future violent behavior insofar as they have analogous drivers, objectives and purported benefits or uses, yet the resulting dangers and implications are socially significant.

First, the facts driving the need to predict violent behavior or identity authenticity coincide. Violent crime and ID theft are threats to the individual and society. Also, prediction techniques are not completely accurate and the public demands for control of these crimes are increasing in number and intensity. Finally, as a result, there is a need for some level of preventative intervention.

As with violence prediction whose objective is to reduce violent crime by predicting a person's potential for inflicting serious bodily harm, identity scoring is aimed at reducing loss that results from fraudulent use of another's identity by predicting whether the applicant identity is reliable or stolen. With violence prediction, the control is a decision to release or imprison a person based on future criminality, while the decision to grant or deny credit benefits is controlled by the authenticity of an applicant's identity.

The problem with both predictive risk situations is a familiar one, that of false positives, where a person is inaccurately labeled dangerous or declared to have dubious identity reliability. The resulting damages on a social level can include statutes, policies and judicial decisions that rely on the seductive illusion of the predictive accuracy, and the use of invalid predictions as a control mechanism for social norms and attitudes. On an individual level, over-prediction can result in denial or violation of civil rights and social liberties, and the criminalization of citizen-victims.

To be sure, predictive technologies can offer insight and knowledge, but the question should be: How should the inferences and gleaned

---

assurances that the credit-seeker is not an impersonator, there is no way to ensure shared risk and commerce will generally collapse. *See* Charles Kahn, *Credit and Identity Theft*, J. MONETARY ECON., *available at* http://www.sciencedirect.com/science/journal/03043932.

knowledge to be used to make decisions in light of ethical and legal considerations?[307] As discussed subsequently, if the proper entities do not know the methodology underlying the results, there is no way to assess how the predictions serve the objectives for which they are being applied. For example, "what is the deterrent value and effect of violence prediction on the crime rate?" can be likened to "what are the loss savings and effect of ID scoring on financial or other fraud?" In other words, without knowledge of the underlying technique and data, how do we know that ID scoring is identifying and reducing identity fraud? Further, absent some reasonable level of transparency and participation in the development and application of the methodology (i.e., which factors to use to improve accuracy or how the methodology can be improved to produce accurate results), identity scoring risks self-reinforcing irresponsible or unaccountable knowledge and resulting actions upon which it is based.[308]

(i) ID Scoring: Handicapping Horses

In our race to get ahead of threats and vulnerabilities associated with IDC, utmost attention must be paid to both the analytical risk models chosen and the data which is fed into those models. Otherwise, the lineage of decisions, perceptions, expenditures, and allocation of resources that spawn from reliance on the accuracy of those risk models will be tainted by the fiction and confusion instigated by the fraudulent identities themselves.

Identity analytics, and specifically, identity scoring, is one of industry's latest responses to the proliferation of IDC. This technique and the entities that build or sustain business models around it are the progeny of the bare-knuckled free market driven policy: information security inefficiencies taking a backseat to information availability efficiencies. In lieu of comprehensive, agreeable IDC statistics the economics of digital identity are about the scarcity of reliable digital identities. Identity scorers are the new suppliers in this market. They are the intermediaries for digital identity artifacts, the new gatekeepers of identity reliability.

307. Keep in mind that decisions reached and spread in digital format are, in many cases, notoriously tenacious to resisting correction. The stories of the poor souls who wind up mistaking place of the TSA flight risk list are but one example of this tenaciousness. *See* Thousands Wrongly on Terror List, http://www.globalissues.org/article/692/thousands-wrongly-on-terror-list (last visited Sept. 2, 2008).

308. Beverly Koerin, Violent crime: Prediction and Control, Crime delinquency, http://cad.sagepub.com/cgi/content/abstract/24/1/49 (last visited Sept. 8, 2008). In general, the methodology involved in predictive analytics involves: 1) Identifying the criterion for the categories of behavior/identity, 2) Identifying the predictor factors, 3) Defining the process for classifying based on behavior/identity artifacts, 4) Testing on a target population the relationship between the criteria and the predictors, and 5) Retesting to cross-validate. *Id.*

ID scorers are playing an increasing role in managing and crafting information from the enormous amount of identity data available electronically. As the technique is applied, ID scoring involves profiling identity artifacts in relation to identity events, behaviors and relationships, creating an identity rating score for a person using analytical techniques, and then selling those scores. If credit scoring attempts to predict the risk that an identified person will not pay off a future debt based on past transactions, identity scoring deals with that same risk by attempting to predict the risk that an identified person is inauthentic, thus inferring that any subsequent debt is likely to go unpaid.

To underscore the gravity of the concerns posed by ID scorers, we analogize identity scorers to public service corporations based on functional similarities.[309] Like railroads to 19th Century industrial society, steel mills to the manufacturing society, and search engines and telecommunications carriers to the information society, identity scorers are private businesses that increasingly control resources with important public implications. Identity scorers also affect broad segments of society, and by proxy wield the power of the markets they serve not unlike that of a public authority.[310]

The most prevalent grievance against public service corporations is bias –inequitable or unfair treatment or refusal to serve some individuals or groups. The problem of bias in identity ranking involves: 1) The choice of data placed in the "ranking machine"; 2) The model or formula applied to that data; and, 3) The nature and weight of the inferences attached to the outcome of the formula. When one or more of these variables is locked up by organizations in the face of formidable public interest in transparency and accountability of the "sausage-making-process," we are left with a black box society, where decisions are made that affect society absent its citizenry having accurate perception and/or participation in the basis for such decisions.

How might this bias be applied? The algorithm which informs the probability of identity authenticity may be dialed to satisfy clients' needs such as maintaining market advantage over its competitors (e.g., to meet Red Flag compliance requirements). The algorithm may also be adjusted

309. We distinguish between "ID scorers" as market entities and "ID scoring" as techniques that may be used by market entities, because of qualitative and quantitative difference in harms and remedies. Since the completeness and theoretical accuracy of one's identity score is directly proportional to the scope of the network activities used to baseline and optimize the results, it is reasonable to conjecture that business models will continue to be built on acquiring and offering access to the "network" rather than just a stand-alone tool.

310. Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, http://works.bepress.com/oren_bracha/1/ (last visited Sept. 2, 2008).

in response to the changing threat model posed by fraudsters, thus altering perceptions about the extent of ID fraud. The results may be manipulated in response to inducements by clients or other influential entities who seek trends that are favorably tied to economic decisions. Finally, results can be skewed to assure the perpetuation of the ID scoring business model. Also, the breadth of the bias can extend universally or locally, which means the range of persons affected can fall anywhere on a spectrum.[311]

The harmful or contentious effects of ID scoring bias are numerous and consequential. The bias in algorithm decisions which generate one's identity ranking carries risk for both the individual as well as the organization making business decisions based on the reliability of that determination. The harms include the undermining of democratic values including fairness and individual autonomy and, ironically, the creation of economic inefficiencies. For example, under the efficient market theory, businesses can only make rational decisions when they have accurate information. A lender bank or insurance company, for example, makes its decision about extending credit, or backstopping health coverage based on information about whether an applicant is who he says he is. If this information is inaccurate (either the results produced are a false positive or false negative) then those decisions and systems fail.

As it relates to individual harm, ID scorers may undermine a person's freedom by threatening the open and equally available opportunity to avail herself of the goods and services upon which it runs. The democratic principles of participation, fairness and individual autonomy, which are guaranteed in our government's interactions with its citizens, have nonetheless migrated to the private sector where there are expectations that companies treat customers fairly. Although not backed by the force of the Constitution, citizens' expectation of democratic values are manifest in legal tools such as consumer protection statutes, freedom of information and public records acts, and private rights of action, not to mention via the invisible hand of the market, where companies are reminded of the force of consumer preferences and the court of public opinion.

Specifically, these principles come into the fore when individuals are denied loans or other credit, or are subjected to higher rates or premiums based on the identity risk score used by the respective financial institu-

311. The very act of ranking presumes the criteria underlying the predictive algorithms carries a decisional bias some identity artifacts have greater importance than others. Optimization involves iteratively tweaking the algorithm and criteria to more closely align the results with the objectives.

tion. Yet, these principles are sidestepped when individuals have no mechanism to access, comprehend, respond to, or participate in the determinations to grant or deny them fundamental tools to survive in our capitalistic society.[312]

What is worse, the ID scorer market is selling its solution implicitly and explicitly to the would-be citizen-victim. The question is whether this market is providing the illusion of control by offering convenience in assessing digital identity authenticity, or, is it reinforcing a lack of control and choice for the individuals behind the digital identities? If the concept of privacy includes an individual's capability to control information about him or herself, the question becomes whether the technological capabilities of identity scoring to create an analysis or "virtual picture" of an individual that is contained in the electronic marketplace violates such person's privacy by supplanting his control over his personal information.[313]

---

312. The risk of lack of oversight and accountability for safeguarding citizens' rights is illustrated by how identity theft service and data providers are able to skirt requirements imposed upon entities covered by FCRA with contractual disclaimer language. In this way, they wield, albeit in informally, the authority yet bear none of the responsibility of entities regulated by FCRA. For example:

> You acknowledge that any information or report which is covered by the FAIR CREDIT REPORTING ACT (public law 91-508, 15 USC section 1681, et seq. subsections 604-615) will be requested and used by the client in full compliance with the terms and intent of that act. The client understands that the purpose of the information purchased as covered by the Fair Credit Reporting Act must be identified, that the information received is for the client's use only, and that there are criminal penalties for willful violation of this act.

Background Check Disclaimer, https://www.efindoutthetruth.com/disclaimer.htm (last visited Apr. 21, 2008).

> I will comply with all applicable laws concerning access to or use of criminal records, and I agree to comply with the federal Fair Credit Reporting Act, 15 USC _ 1681 et seq. I agree to hold harmless the provider of this service, its officers and employees, from any expense or damage resulting from th publication of information provided by this service."

abNC, Disclaimer, http://www.abcnc.com/Disclaimer.aspx (last visited Apr. 21, 2008).

> Further, I will not, either personally or through my company, employer or anyone else, use this information for credit granting, credit monitoring, account review, insurance underwriting, employment or any other purpose covered by the Fair Credit Reporting Act, 15 U.S.C. Sec. 1681 et seq, ("FCRA"), Federal Trade Commission interpretations of the FCRA, and similar state statutes.

FCRA Disclaimer, http://www.findpeople.org/infoquest/Disclaimer.html (last visited Apr. 21, 2008).

313. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482-83 (1968) [hereinafter Fried]; Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 281 (1977) [hereinafter Gerety] Professor Fried argues that a "person who enjoys privacy is able to grant or deny access to others" of information about him or herself. Fried, *supra,* at 482. Professor Fried uses the example of a house to explain his point. *Id*. at 483. One's house is private because the law allows individuals to exclude others from the house, and the "house is constructed - with doors, windows, window shades - to allow it to be made private." *Id.* Professor Fried also makes a distinction between simple control over the quantity of information and con-

Opponents of this position may argue that fairness norms have no placemat at the free market table.[314] Courts and regulators, however, have been more amenable to applying fairness and accountability norms to private companies when affected persons have no alternatives or way to "exit."[315] Specifically, ID scorers are on the cusp of occupying a significant place of power insofar as their identity scoring decisions liken to become pivotal to whether individuals obtain credit and derivative goods and services. This is true to the extent that they reach minimum thresholds of participation by financial services, insurance, real estate, e-commerce, government and retail institutions, which rely on their analyses to prevent loss from ID fraud.

More importantly, industry clients are incentivized to patron the ID Scorers with the largest client base, thus perpetuating the network effects of having all identity proofing controlled by a few entities. Each additional company that contributes to the pool of ID artifacts by joining the network theoretically decreases the cost of better predictions that result from optimization (algorithm tuning) based on this new data.[316] In this sense, citizen consumers will have no input in choosing, lest avoiding identity vetting by one or a few private entities. The ability to

---

trol over the quality of the knowledge. *Id.* "We may not mind that a person knows a general fact about us, and yet feel our privacy invaded if he knows the details." *Id.*

Professor Gerety argues that "[p]rivacy is . . . the control over the autonomy of the intimacies of personal identity." Gerety, *supra* at 281. Professor Gerety distinguishes privacy from confidentiality. *See id.* at 282. Private information "excludes all but such information as is necessary to the intimacies of our personal identities." *Id.* Confidentiality, however, is created through either "implicit or explicit mutual agreement" and does not depend on the type of information. *Id.*

This concept of privacy as an individual's capability to control information about him or herself has also been referred to as "database privacy." Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS J. 555, 556 (1998). Professor Schauer defines "database privacy" as "the purported right of individuals to control the distribution and availability of information about themselves that may appear in various governmental and nongovernmental databases." *Id.*

314. The option to voice change in the market as a way to reform or protest is comparatively credible as exiting the market. Hirschman, Exit and Voice: an expanding sphere of influence, Rival Views of market Society and Other Recent Essays 55 (Elizabeth Sifton Books) (1986). In fairness, there are legitimate arguments based on intellectual property rights and public interest that support some level of protection of ID scoring algorithms. *Id.* Full, public transparency could be detrimental to the quality of the ranking since knowledge by fraudsters may enable them to manipulate their tactics in using the stolen identity artifacts. *Id.* This gaming could also magnify structural biases of ranking algorithms in favor of certain institutions. *Id.*

315. Bracha, *supra* note 97, at 289.

316. Optimization involves iteratively tweaking the algorithm and criteria to more closely align the results with the objectives.

enter into meaningful agreements will be an illusion at best.[317]

Second, the deleterious effect on individual autonomy is a related potential harm flowing from ID scorer bias. As Charles Taylor expressed in *What's Wrong with Negative Liberty*, autonomy encompasses more than the absence of constraint, but rather, involves a meaningful variety of choices, relevant knowledge of societal context, and alternatives, and the capacity to evaluate and make a choice among options. So, applying the adage if "A controls the window through which B sees the world then the autonomy of B is diminished," ID scorers will increasingly control the flow of information about individuals' identity authenticity in ways that shape and constrain their choices by passing judgment to institutional decision makers and eliminating access to that flow of information to the subjects of those determinations. The citizen applicant sees only the rejected application with a minimal and abstract reasoning couched as objective criteria for denial. The intervention and significance of the role played by the ID scorer in making this determination is neither transparent nor increasingly avoidable.[318]

---

317. We acknowledge the counter-argument: practicality and efficiency demands that we cannot afford to have a system that allows individuals, per occurrence, to negotiate with institutions; and, that people actually do not want to contract individually because they are not knowledgeable enough to make the best decision for themselves and/or don't want to hassle with it. The existence proof of the counter-argument to this posture is the European Union, which allows citizens control over such data.

318. *See, e.g.*, Beck, *Credit Scores Hit by Card Limits,* http://news.yahoo.com/s/ap/20080628/ap_on_bi_ge/all_business (last visited Sept. 8, 2008).

> Card companies are reducing borrowing limits for tens of thousands of consumers, which then can lead to lower credit scores. Those facing this predicament might not even know it until they apply for a loan or another credit card, and then get denied because their credit score has dropped. This is an unintended consequence of the financial world's widespread ratcheting down of risk. Banks and other card lenders are trying to better protect themselves from more massive losses like those they've seen from subprime mortgages. As a result, they are looking for ways to reduce their exposure to cardholders more likely to default. . .. Here's how that happens: Let's say a cardholder has a credit limit of $10,000 and a balance on the card of $4,000. The card company worries that large balance may increase the prospects for default, so it lowers the credit line to $5,000. But in doing that, it completely changes what is known as the credit utilization rate, raising it from 40 percent to 80 percent. That is then factored into the calculation of one's so-called FICO credit score, which measures creditworthiness, according to Craig Watts, a spokesman for FICO-creator Fair Isaac Corp. A lower FICO score could make it more expensive for someone trying to borrow money. For instance, someone taking out a $25,000 36-month auto loan would see an interest rate of about 6.4 percent and a monthly payment of $765 if they were in the highest range of FICO scores of 720 to 850, according to Fair Isaac's Web site, myFICO.com. That then jumps to an interest rate of 7.3 percent and a monthly payment of $776 for those with a score of 690 to 719 and as much as 15 percent or $866 a month for those with the lowest FICO range of 500 to 589. According to the Comptroller of the Currency, one of the government agencies that regulate U.S. banks, companies must notify cardholders at least 15 days in advance before making changes in the terms of their account, such as lowering the credit limit. But they don't have to explain how that could

Another contentious effect of ID scorers is that by having concentrated control over the flow of information (i.e., good and bad identity artifact profiles) and the ability to manipulate it, economic inefficiency and stifled competition may result.[319] In other words, we may face the ills that beset monopoly regimes. The argument here is that ID scorers are acting as gatekeepers of identity reliability and can use this position to increase or decrease the pool of "authentic" identities who want to engage in the credit (or other system predicated on identity authentication) system, thereby limiting competition among client institutions by skewing information flows or stifling innovation or other "value generating" solutions by disincentivizing investment in other providers of ID authentication. For example, Acme Bank may have disproportionately higher numbers of alleged fraudulent applicants compared to its competitor Beta Bank, and thus it does not extend as much credit, and reap the derivative effects that flow there from.

Finally, perhaps the most perilous consequence of reliance on a closed system of identity scoring is the relative inability to undo an erroneous judgment has been acted upon. Take, for example, a common scenario where a person is denied a loan because of a low ID score and such determination is reported to any number of institutions associated with the transaction, such as consumer credit bureaus. If the information was fed into the algorithm or the algorithm configuration itself is later determined to be inaccurate, even assuming a correction and proper decision by the company directly relying on the conclusion were made, the likelihood all downstream recipients of and actions predicated on initial information will be retracted is a pipedream, at best. To paraphrase an adage, "the toothpaste is out of the tube and it's not going back in." This erroneous reliance on flawed information is what spawns the pollution of that identity, for it cannot be retracted and will continue to be associated with such individual when she attempts to establish credibility with any number of market participants who act on the reliability of that original pronouncement.

(ii) Identity Analytics –Case Example

We insert some teeth into the risk analysis of identity scoring within the context of our current ID Theft crisis by turning to first-source findings produced by a market-leading identity scorer company. ID Analytics, retained by various high profile corporate victims of database

> change an individual's credit score. That puts the burden on consumers to watch out for this. They better so they don't get blindsided.

Id.

319. *See* Oren Bracha & Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the law of Search*, http://works.bepress.com/oren_bracha/1/ (last visited Sept. 2, 2008).

breaches professes to have conducted the only national database breach study. Since knowledge about the dynamics of their methodology and data is undisclosed, we rely on statistics and conclusions rendered in its two major publications on the subject, *The National Data Breach Analysis* and *The Data Breach Harm Analysis*, along with news media reports and conference pronouncements.[320] It is upon this corpus of information we highlight several contentious analyses and the real consequences that may flow as a result.

The bias in these conclusory findings is manifest more so in what is not stated, but what is inferred, rather than what is explicitly imparted. For example:

- The highest rate of misuse of PII compromised in a data breach was 0.098 percent.
- Criminals are limited by practical considerations when using stolen IDs. This suggests that the smaller the intentional data breach, the higher the identity theft risk posed to the individual consumer impacted by a data breach.

It bears dissecting these claims to see a different perspective of the truth behind the analyses. For one, this analysis covers only one type of IDT –the directly financially motivated, variety, which is only a slice of the pie. It does not address the other types of IDT such as healthcare/ medical, immigration, terrorism, or criminal IDT. Within the category of financially motivated IDT, it only addresses credit card application fraud. Again, this is only a percentage of the subsets of financial IDT such as fraudulent use of ATM/Credit Card, forged checks, fraudulent tax returns, or acquisition of additional identity documents like breeder documents such as Driver's License, Passport, Identification card, etc.

Third, the conclusions only encompass that single type and single subset of IDT, which are limited to its proprietary network of clients, which include the likes of financial institutions, retailers, utilities, and auto dealers. IDA's conclusions are based on an assumptions if the identity artifacts are not: (1) manifest in a fraudulent credit application; (2) inside the limited realm of its network of clients; and (3) within the immediate aftermath of a breach or within a maximum of six months, then a person is deemed to not be at risk of having his identity stolen. Yet, in light of the facts that there is an underground market which thrives on trade in ID artifacts, identity artifacts are relatively permanent,[321] and, aboveground commercial transactions anchor on identity artifacts (which

320. ID Analytics National Data Breach Analysis, *The Data Breach Harm Analysis*, http://www.idanalytics.com/whitepapers/ (last visited Sept. 18, 2008).

321. The artifacts we use to identify and often authenticate are relatively static across time and difficult to change. This is significant feature of our notion of identity- permanence and fixity, which similarly is an assumption upon which our propositions in this paper are based.

means artifacts have staying power in the marketplace), there is very little supporting the notion the artifact will not be resurrected and used fraudulently across time and space. In other words, given the conditions above, there is no predicting one's identity artifact(s) will not be used fraudulently at the local bank or in a mortgage transaction across the world, within a week, six months, or several years.

To dissect further, applying basic math and reasoning to what is disclosed by IDA only reinforces concern for how the undisclosed data is sliced to justify its findings and conclusions. For instance, encompassing complete coverage of all United States identities juxtaposed with pronouncements about handling three billion identity artifacts means that at best, their probabilities are based on at most 750,000 people, which flies in the face of common knowledge let alone United States Census records about the number of persons in the United States.[322]

So what is the significance of the skewed analyses we underscore, in light of harms we described in the previous section-biased results, diminished personal autonomy, stifled competition and lack of control over one's identity? From a legal risk and responsibility perspective, courts are requiring manifestation of damages in lawsuits and breached companies are required to justify decisions to notify or not based on standards of "reasonable likelihood." Identity analytics is being relied upon to support conclusions about whether the identities in the breach have been compromised based on ID scoring techniques and networks. In light of the black box approach to disclosing what data and model companies like IDA uses to reach conclusions,[323] which involves more than just studying the data involved in the breach, it is difficult to determine how and to what extent the IDA conclusions are being used.

The bias risk is real and apparent, insofar as companies offering this type of analytical conclusion stand to profit from their opaque ratings and self-fulfilling prophecies. This is especially so given we suggest identity scoring is a logical complement and evolution of credit risk scoring. Although not widely publicized, the checks and balances on such bias risk in the credit arena are loose at best. If creditors have no duty to consumers to ensure the accuracy of the analytical scoring upon which they rely, then certainly the companies doing the ratings are under no legal obligation to provide empirical and objectively accurate analytical results.[324] Within these liability gaps, then, lies fertile ground for ana-

322. This calculation is based on four artifacts per person, and this figure is liberal because we assume that all applications analyzed were from distinctly different persons.

323. The justification being that such transparency would undermine trade secrets.

324. Baker v. Capital One, 2006 U.S. Dist. LEXIS 62053, No. CV 04-1192-PHX-NVW (D. Ariz. Aug, 28, 2006). The court, however, has already determined that 15 U.S.C. § 1681s-2(b) does not by its terms require creditors to report consumers' credit limits. *Id.* Granted, a creditors' choice not to report its customer's credit limits may negatively effect

lytics companies to sow seeds that are beneficial to their corporate customers.

Nevertheless, there is no speculating that implicit in their reported conclusions about the scope and prevalence of IDT, is that the breached identities have in fact been "compromised." ID Analytics uses the fact that all or part of the breached identity was used in an attempted account opening as the basis for its conclusions on the likelihood of an identity being misused, or "compromised." Yet paradoxically, these allegedly compromised identities are not being recognized by courts as having been misused as illustrated by the previously discussed jettisoning of data breach lawsuits for lack of damages. If ID scoring is used to support a denial of services or financial benefits, why are those same conclusions not being used to support damages requirements for citizens whose identity has been compromised in a data breach?

Breached businesses are seeking methods by which to gauge the notification trigger: whether or not the breach has resulted in a reasonable likelihood of a harmful outcome.[325] The trigger standard, which dictates whether they are required to notify, is a mandate that has nontrivial economic ramifications. In light of the confusion and uncertainty in applying the standard, it is reasonable to suspect an identity risk scoring solution may be implemented to decide if the breached identities should be notified, or to support or refute damage assessment, or even to gauge compliance risk in the normal course of business before a breach occurs.

Such an application is already occurring in the realm of compliance with a related mandate, the Red Flag Regulations mandated by FACTA which go into effect in November, 2008.[326] These federal regulations

---

those customers' credit scores, if calculated using FICO methodology. But third party use of a possibly imperfect methodology in synthesizing consumer information for commercial use does not give rise to a legal duty, previously unrecognized, requiring creditors to cater their reporting to such third party's methodology. Baker has provided no authority for the proposition that creditors bear responsibility for assuring that FICO score generators render "accurate" results when inputted with otherwise accurate reported information. *Id.* Rather, the legal duty of creditors to report information in response to disputes is governed by 15 U.S.C. § 1681s-2(b), which includes no specific requirement that credit limits be reported by creditors who do not ordinarily do so. *Id*.

325. The trigger standards for notification vary across states. In general, they break down along some combination of 'use risk' and corresponding 'outcome'. Use risk includes: reasonably-possible, reasonably-believed, risk, reasonably-likely, likely, material risk, substantial risk, significant risk, substantial risk; and outcome includes: breach, misuse, criminal activity, illegal use; harm, loss/injury, economic loss, ID theft/fraud.

326. The regulations and guidelines implement sections 114 & 315 of the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (FACTA) (codified at 15 U.S.C. §§ 1681m(e), 1681c(h)). The final rules requires each financial institution and creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement a written

mandate all creditors –financial institutions, retailers, utilities, and auto dealers that extend consumer credit or hold consumer accounts. The purpose is to develop and implement a proactive Identity Theft Prevention Program. For instance, ID Analytics product, "ID Analytics for Compliance" is touted as a product solution for entities that come within the scope of the Rules:

> Today's consumers face a wider variety of identity fraud threats than ever before. Businesses must do their part to protect against identity theft while maintaining a high quality, seamless business experience for legitimate consumers," said Todd Higginson, director of product marketing, ID Analytics, Inc. "By resolving Red Flags without manual intervention, ID Analytics for Compliance minimizes the use of time-consuming review processes that drive customers away. Technologies that detect and do not resolve Red Flags will create problems, not solutions, for creditors[327]

There is strong reason to believe, given the cost-prohibitive and intractable reality of compartmentalizing the spread of electronic information once it is exposed in our internetworked environment, organizations will turn to probabilistic statistics about the rate of misuse to inform its self-certifying conclusions that breach notification has not been triggered. Similarly, it is not implausible to believe that a secondary use of this analysis will inform legal determinations about future damages for IDT victims who exercise private rights of action. In other words, will standards for breach notification and damages devolve into probabilistic-guesswork, rather than the causal-determinism upon which our legal system is based? Given the lack of transparency in methodology, data, and statistical significance of the findings as it relates to the appropriateness of applying these probabilities to dissimilar fact patterns, strong caution should be the beacon when engaging in decision making based on these analytical conclusions.

As for diminished autonomy risk, the algorithms used by identity scorers establish one's rank relative to others in the respective data network. Consequently, not unlike the use of algorithms in search engine page ranking to affect how high a website is listed in search results, it is

---

Identity Theft Prevention Program for combating identity theft in connection with the opening of new accounts and the maintenance of existing accounts. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63,718 (Nov. 9, 2007) (promulgated jointly by several agencies and codified in various parts of the C.F.R.). The Program must include reasonable policies and procedures for identifying "red flags" that will help detect, prevent, and mitigate identity theft. *Id.*

327. ID Analytics, Press Release: ID Analytics for Compliance Enables Creditors to Satisfy Red Flag and Address Discrepancy Compliance Without Impacting the Consumer Experience (May 7, 2008), *available at* http://www.idanalytics.com/news_and_events/20080507.html (last visited May 7, 2008).

easy to comparatively conclude how individuals can be unfairly graded in a creditors search for high-ranking identities. From a business perspective, this has resulted in lawsuits over significant revenue decline. From an individual's perspective, similar damages result in lost opportunity costs or other even less tangible or traceable harms.[328]

A final harm from loss of control over one's identity is the danger it cannot be remediated or cleaned up. The identity scoring may in fact be beneficial insofar as this is used as one part of the multiple streams of corroborating evidence for authorization, but what about when those artifacts become so numerous and polluted with associated artifacts that are inauthentic –a likely possibility given that we are increasingly leaving digital identity traces all over the World Wide Web and associated digital environment? The seminal questions are: What is the standard for determining identity authenticity? Who gets to decide between competing and conflicting artifacts. Finally, what confidence levels will be required when the decision making is automated?

To be sure, identity analytics products may very well be useful to businesses seeking to reduce compliance and other digital risks. However, the corresponding risk to citizen-consumers must be considered and balanced in kind. As these automated products and services are proliferating, relied upon and embedded in business processes to address the challenges of information risk, citizens and elected representatives deserve to understand the ramifications, both beneficial and harmful. As with any attempt to assess and balance interests, effective policy should demand life-altering decisions affecting citizen-consumers should not be strong-armed by an unregulated free market which eschews knowledge, disclosure and consent by citizen-consumers.

III. DIGITAL SECURITY AND CYBERCRIME IN THE U.S.: THE LEGISLATURE AND FREE MARKET[329]

328. Comparative examples of the hidden and nebulous harms that result from decisionmaking via the market manifest by way of the use of automated algorithms in business decision-making. For example, in a recent book, John Battelle presents the story of the owner of 2bigfeet.com (a seller of large-sized men's shoes). The site fell off the first page of Google's rankings after a change in Google's algorithm in November 2003, just before the Christmas season. The site's owner could not get a response from Google. See John Battelle, The Search: How Google and its Rivals Rewrote the Rules of Business and Transformed our Culture 157 (2005). Similarly, KinderStart.com, a search engine devoted to information about parenting, unsuccessfully sued Google, claiming anticompetitive behavior, after KinderStart.com dropped to a "zero" ranking. Anne Broche, *Judge Favors Google in 'frivolous' Suit*, CNET NEWS, Mar. 20, 2007, http://news.cnet.com/8301-10784_3-6168999-7.html.

329. Broadly speaking these terms represent two sides of the same coin. The difference between the terms, cybercrime v. digital security issues can best be described as one group

A. The Battle for Policy Control: Omnipresent Challenges

Drafting laws and regulations to address privacy, digital security, IDC, and cyberspace issues in general present unique challenges. The same is essentially true for interpreting the laws and implementing the regulations eventually adopted. This subsection addresses how some of these challenges have been dealt with and their implications for the creation and protection of the digital persona.

Congress and courts in the U.S. must have better information before they can craft effective laws in the area of privacy and digital security. Unfortunately, our legislative and judicial institutions are operating in the same information vacuum in which many researchers and businesses are operating: an acknowledged lack of reliable metrics upon which to craft policy decisions. Even a cursory outlining of some of the principles which underlie our information society underscore the unique challenges policy makers and implementers face regarding PII collection, management and disposition:

- Decentralization: time and space problems create information gathering and jurisdictional issues.[330]
- Anonymous actions: the nature of the Internet protocol renders anonymity the default state in the digital realm.
- Interdependence: problems in one place effect all places.
- Electronic information: electronic data is the lifeblood of our Internet and web environment, inures a feature set orders of magnitude different than its paper-based ancestor along the spectrum of collection, storage, transmission and security.It is much more easily searched and discovered, collected, copied, disseminated, and manipulated without detection. It is these features upon which the Information Revolution is based.

The new context presented by the digital environment confluences with a pervasive effort on the part of many entities to underreport security incidents in the first place. The relevant data upon which to base sound analyses is hard to aggregate, is prone to imperceptible manipulation after capture, and generally the knowledge extracted from the data is closely guarded and not widely disseminated. This leaves society relying more and more on anecdotal evidence, self-reporting surveys, gossip and rhetoric, and reinforces legal and social fictions.

---

trying to create, steal, corrupt, or manipulate data for criminal or wrongful purposes. The other side is trying to protect the integrity and privacy of digital data.

330. In essence, data can both exist and spread anywhere across the physical Internet and related virtual World Wide Web, which makes its reach potentially both global and ubiquitous. Jurisdictions are steeped on physical geography, which are meaningless in our Internetworked society. For instance, when an American consumer purchases goods from German website, what consumer protection statutes govern transaction?

The object in previously highlighting and examining the FTC IDC figures was not to dump derision on the FTC, or many of the other surveys. The larger point in examining the figures was two-fold: first, to highlight the difficulty society and the legal and legislative systems have encountered wrestling with technical, managerial and socio-legal barriers to integrating, correlating and interpreting cybercrime; and, second, to show how these barriers corrupt the analytical process leading to the drafting and implementation of law and regulations affecting IDC. This means society and its institutions are placed in the difficult and potentially dangerous position of knowing increasingly less about an environment where we conduct more and more business transactions, governmental interactions, and actions relating to personal life.

The preceding section suggests how ambiguity over cause, value and loss, and risk are rampant enough to justify any parties' position such governance of these issues –liability, privacy, credentials, fraud, burden, incentives– carries a high risk of inaccuracy. We cannot adequately answer questions related to how identity is wrongfully acquired and used without better actuarial data on the crime. Yet Congress has the challenge of fashioning legislation to govern cyberspace. This subsection will briefly examine some of the specific challenges and briefly identify some of the possible responses Congress is contemplating.

B. The Legislative Response: Congress to the Rescue?

If, as we posited in the last few paragraphs above, the risks of imposing a legislative, regulatory, or judge-made mandate are high absent reliable data on IDC, what might society request the judiciary or legislature to do in the face of chaotic digital environment. Borrowing from the Hippocratic Oath, at a minimum, we could ask them to "do no harm."

We suggest the courts, especially, have "done harm" in the realm of data breach notification jurisprudence. Congress' record is murky, but incomplete at this point. However they appear to be leaning in a direction, which would potentially do significant harm to efforts to protect the digital PII of Americans. Interesting enough, the regulatory agencies deserve the most commendation for trying to establish rules to protect digital PII in this new environment however, the regulatory agencies have been swimming against the congressionally-mandated anti-regulatory tide of the last twenty-five years or so. This is especially so in areas of strong market bias, such as digital security and digital identity management. There are indications Congress is contemplating turning over the key area of data breach notification regulation to free market forces. If this becomes a reality, we contend it will be a profound mistake with far reaching ramifications. As it stands currently, there is a strong argument that the government has already conceded control of identity to the

free market by facilitating policies of initiatives that disincentivize security. It is the evolution of these legislative policies that we now turn.

The headlines of digital insecurity jump at us on an almost daily basis:[331] "Insider Pilfers Customer Database," "ID Theft is the Fastest Growing Crime in America", "Corporate Laptop with Customer Data Stolen", "University Database Hacked Into." Further, this explosion of publicity comes in the wake of the passage of numerous laws supposedly intended to protect citizens from privacy violations and cybercrime.[332] Given the high profile media attention paid to IDC, in the wake of the passage of all these privacy laws it is understandable if the public perception was personal data is being managed insecurely.[333] No law catalyzed this posited public perception better than the flagship database breach notification law in California –Senate Bill 1386.[334] Before going into effect in 2003, the American public was relatively unaware of the extent data breaches may have been occurring.[335] Indeed, the public was essentially lacking any mechanisms that might heighten their awareness in the first place.

It is now commonplace to hear about data breaches, aided certainly by the bandwagon of state notification laws.[336] Although the panoply of sector-based laws first heightened perceptions of privacy and data secur-

331. New breaches come to light on almost a daily basis. *See* Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm (last visited Sept. 1, 2008).

332. *See* 1996 Fair Credit Reporting Act ("FCRA") revisions, Consumer Credit Reporting Reform Act, 104 Pub. L. 208, 110 Stat. 3009 (1996) (codified as amendments to FCRA beginning at 15 U.S.C. § 1601); Identity Theft and Deterrence Act of 1998, Pub. L. No. 105-318, § 4, 112 Stat. 3009, 3009 (1998) (ID Theft Act); The Graham-Leech-Bliley Financial Modernization Act ("GLB"), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 U.S.C. and elsewhere); Health Insurance Portability and Accountability Act of 1996 ("HIPPA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996); Sarbanes-Oxley Act of 2002 ("SOX"), Pub. L. 107-204, 116 Stat. 745 (2002) (codified at 15 U.S.C. § 7201); Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. §§ 1681m(e), 1681c(h)).

333. By "managed", we refer to the lifecycle of information- collection, storage, processing, accessing, transmission, and use.

334. S. 1386, 2002 Cal ALS 915 (codified as amended in CAL. CIVIL CODE §§ 1798.29, 1798.82), *available at* http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html.

335. If we look, for example, at the Dataloss data, we see that reported incidents averaged about one per month until early 2005. Open Security Foundation, DATALOSSdb, http://datalossdb.org/ (last visited Sept. 1, 2008). Obviously, if data breaches were not being reported, the public would not be aware of the problem. It is certainly debatable to what extent the steady increase after 2005 of reported incidents was a function of new notification laws, and to what extent the increase reflects an increase in actual incidents.

336. Forty-nine states now have data breach notification statutes. *See* PIRG, State PIRG summary of state Security Freeze and Breach Notification Laws, http://www.pirg.org/consumer/credit/statelaws.htm (last visited Sept. 1, 2008).

ity, it was the notification element of the breach laws that cemented the logical link between increased awareness of data insecurity, the vulnerability of digital data, and ultimately, the perceived explosion in IDC. And it is this area of digital insecurity, DBN legislation, or lack of said same, we have come to see as the most crucial question, at the moment, facing society in preventing the emergence of chaotic digital environment and all the potential devastating consequences such scenario conjures up.[337]

On one level the U.S. seemed to move into the digital age in the blink of an eye. Most consumers were without personal computers or at least, without access to the Internet prior to 1995.[338] However, things began to change dramatically in 1995 with the introduction of the first Internet browser. It was around this time that the reports of what we have come to call ID theft began to dramatically increase.[339] Precisely because of the lack of authoritative statistics on ID theft it is difficult to measure exactly when this explosion of ID theft began. There are however certain, anecdotal, clues:

1. No Law Review Articles on ID theft prior to 1999;
2. No federal laws employing the term, ID theft prior to 1998;
3. Not a mention of ID theft during the 1996 Revisions of FCRA; and
4. No state laws employing the term ID theft till 1996.

To be sure, there is validity to the claim the "epidemic" is caused in part by the increased reporting of incidents, which had been occurring

337. Two recent stories in the media highlight the direction, perhaps thoughtlessly, that society is moving with regard to a chaotic digital environment. One story notes that school lunches are now being paid for by students providing their fingerprints into a digital scanning device, which in turn passes the data into a larger data based that records the transaction. Wylie Wong, *Biometrics Goes to School*, EDTECH, http://www.edtechmag.com/k12/issues/june-july-2006/biometrics-goes-to-school.html (last visited Sept. 1, 2008). Papa Ginos' pizza chain is essentially doing the same thing. Paul Korzeniowski, *Papa Gino's Goes Biometric*, DARK READING, May 16, 2008, http://www.darkreading.com/document.asp?doc_id=154109&WT.svl=news1_4. Contemplate what the consequences might be if this digital treasure trove is breached? We will never be able, or at least, not in the foreseeable future, be able to change our bio metric data. Once breached this data will be, forever, susceptible to future misuse.

338. The Internet worldwide had about sixteen million users in 1995. *See* Internet World Stats, Internet Growth Statistics, http://www.internetworldstats.com/emarketing.htm (last visited Sept. 1, 2008). In 1995, there were only about 120,000 internet domains. Robert Hobbes Zakon, Hobbes' Internet Timeline v3.3, Growth, http://www.nic.funet.fi/index/FUNET/history/heureka/HIT.html#Growth (last visited Sept. 1, 2008). Just two years later, in 1997, the number was an order of magnitude greater, or about 1.3 million hosts. *Id.*

339. *See, e.g.,* Sean B. Hoar, *Identity Theft: The Crime of the New Millenium*, 49 UNITED STATES ATTORNEYS' USA BULLETIN, Mar. 2001, http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm.

for some time.[340] However, the more important issue here is whether the upswing in ID thefts is directly related to the dramatic increase in the commercial and online use of digital data. Society began to slowly respond to this emerging problem with a series of new laws, or re-interpretation of old laws. Specifically:

1. ID Theft Assumption and Deterrence Act;[341]
2. Civil Remedies granted under the federal Computer Fraud and Abuse Act;[342]
3. HIPAA;[343]
4. Financial Services Modernization Act 1999 (GLB);[344]
5. Section 5 FTC actions;[345] and
6. FACTA.[346]

This legislative reaction was a sector-by-sector regulatory regime. Banking, medical records, general business records, and credit reports, were each assigned specific legislation and/or regulation. This reaction was immediately undercut because the regulations were so toothless, and weakly enforced the practical effect was a laissez-faire approach.[347] This is especially so when juxtaposed with many other nations experience with this issue.

The Europeans opted for a comprehensive data protection law, Directive 95/46/EC was passed in 1995.[348] It addressed the protection of individuals with regard to the processing of personal data and on the free

340. *See* Kris Erickson & Philip N. Howard, *A Case of Mistaken Identity? News Accounts of Hacker, Consumer, and Organizational Responsibility for Compromised Digital Records*, 12 J. OF COMPUTER-MEDIATED COMM. 5 (2007), *available at* http://jcmc.indiana.edu/vol12/issue4/erickson.html ("[T]he bulk of the reports occur in 2005 and 2006, after legislation in California, Washington, and other states took effect. There were three times as many incidents in the period between 2005 and 2006 as there were in the previous 25 years.").

341. Pub. L. No. 105-318, § 4, 112 Stat. 3009, 3009 (1998) (ID Theft Act).

342. Act of Sept. 26, 1914, ch. 311, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. §§ 41-58 (1994)).

343. Pub. L. No. 104-191, 110 Stat. 1936 (1996). It may be interesting to note that HIPAA was not enacted for privacy and security reasons, but rather, for efficiency purposes.

344. GLB, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified in scattered sections of 12 U.S.C. and elsewhere).

345. 15 U.S.C. § 45 (2006).

346. FACTA, Pub. L. No. 108-159, 117 Stat. 1952 (codified at 15 U.S.C. §§ 1681m(e), 1681c(h)).

347. The first fine ever assessed by Department of Health and Human Services was issued in July of 2008. HIPAA was enacted in 1996. The Privacy Regulations went into effect in 2003. *See* Case Examples and Resolution Agreements, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html (last visited Apr. 21, 2009).

348. Commission Directive 94/46/EC of 13 October 1994, amending Directive 88/301/EEC and Directive 90/388/EEC in particular with regard to satellite communications.

movement of such data.[349] The Directive granted EU resident's property and privacy rights in their data. Therefore, entities holding the data in question had to develop policies and procedures to take, ostensibly, reasonable and appropriate steps to see these rights were not trampled or abused.[350]

The American response, on the other hand meant the same political battles for data and privacy protection are fought anew, sector by sector. This piecemeal approach meant there were different standards, directives, and penalties for each sector. This was the status until the introduction of the data breach notification laws began to allow society to grasp how well, or poorly, the legislation designed to protect PII was working.

Initially, DBN legislation was driven by state law, with California taking the lead in 2003, followed over the next few years by some 40 states passing like-minded laws. The one IDC area where the federal government did chime in with national legislation was the aforementioned FACTA legislation which revised the Fair Credit Reporting Act.[351]

However at present, the main battle being fought in the Congress concerning privacy and ID theft lies with the proposed federal data breach notification law. Various[352] versions of these laws are being considered by Congress.[353] On its face, this move towards federal legislation can be viewed as a shift away from a market-oriented solution to IDC, but the practical effect of the contending bills would be one of the most significant Congressional moves toward laissez-faire protection of PII and IDC. This is because such legislation would place ultimate discretion for defining IDT, determining when and how it occurs, deciding how to best prevent it, and determining who is responsible, with the very

349. Japan passed a similarly comprehensive law; the Personal Information Protection Law, in 2005. Act on the Protection of Personal Privacy, Law of 57 of 2003, translation *available at* http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf.

350. It is worth noting that, while causal determinations are murky, the fact seems to be that the nations covered by the EU Directive are not experiencing the ID theft problems the US is. *See, e.g.,* Liz Pulliam Weston, *What Europe Can Teach Us About Identity Theft*, MSN MONEY, http://moneycentral.msn.com/content/Banking/FinancialPrivacy/P116528.asp (last visited Sept. 1, 2008); Kieran Glynn, *Ireland: Identity Theft Be Cautious or Be Caught,* MONDAQ.COM, http://www.mondaq.com/article.asp?articleid=35504 (last visited Sept, 18, 2008).

351. 15 U.S.C. §§ 1681m(e), 1681c(h) (1952).

352. *See, e.g.,* Clifford Davidson, *110th Congress Proposes Sweeping Federal Data Security Legislation*, Proskauer Rose PRIVACY LAW BLOG, Mar. 6, 2007, http://privacylaw.proskauer.com/2007/03/articles/security-breach-notification-l/110th-congress-proposes-sweeping-federal-data-security-legislation/.

353. Privacy Law Blog, http://privacylaw.proskauer.com/tags/legislation/ (last visited Sept. 18, 2008).

entities who control the information and suffer the breach. As noted previously, damage assessments (the decision whether to publicly announce that a data breach has occurred, and whether a duty to notify the effected consumers has been triggered) will reside with the same entities who have a powerfully vested interest in downplaying the public perception that IDC is occurring.[354]

This posture by the private sector was not always so. At one time the same corporate entities opposed a federal DBN law[355] and the various state DBN laws as an unnecessary regulatory intrusion into their business models. However, as more state laws passed, many with pro-consumer provisions,[356] the corporate entities did an about-face on the utilitarianism of a federal law and almost unanimously,[357] the pending bills called for the federal law to preempt all state laws. The consequence is that consumer-friendly provisions of the state laws like private rights of action, statutory damages, and reasonable legal fees would be jettisoned by the proposed federal law. We contend that if this comes to pass we may experience a reversal of consumer notification, and not as a result of increased security controls resulting in less data breaches, or as a result of a decreased threat to PII.

It is beyond the scope of this Article to cover the textual nuances present in all the bills before the Congress. However, given the impor-

354. At least in so far as those entities are not in the market for selling products or services, or both, to prevent, or respond to, IDC. Jaikumar Vijayan, *Critics Hit Proposed Data Breach Notification Law as Ineffective,* COMPUTERWORLD, Nov. 10, 2005, http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,106116,00.html; Keith Regan, *Can Legislation Stop Identity Theft,* TECHNEWSWORLD, Mar. 1, 2006, http://www.technewsworld.com/story/49099.html?wlc=1220355058; Chris Soghoian, *Industry Giants Lobby to Kill Pro-Consumer Data-Breach Legislation,* CNET, Feb. 5, 2008, http://news.cnet.com/8301-13739_3-9865076-46.html.

355. S*ee* Ryan Singel, *No Fed Security Laws, Hurrah!!* WIRED, Oct. 10, 2005, http://www.wired.com/politics/law/news/2005/11/69525 ("Though banks and data brokers have long opposed federal privacy legislation in favor of self-regulation, both industries are now asking Congress to step in to create a single national standard and cap the limits on their liability in case of a breach.").

356. Statutory damages, right of private action, and reasonable legal fees, among other provisions.

357. Of the proposed legislation, only two bills have been reported to the Senate: the Personal Data Privacy and Security Act of 2007 and the Notification of Risk to Personal Data Act of 2007. Bills before the House include: Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Data Security Act of 2007, S. 1620, 110th Cong. (2007) (mirroring H.R. 1685); Cyber-Security Enhancement and Consumer Data Protection Act of 2007, H.R. 836, 110th Cong. (2007); Personal Data Protection Act of 2007, S. 1202, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007); Personal Data Privacy and Security Act, S. 495, 110th Cong. (2007); Notification of Risk to Personal Data Act of 2007, S. 239, 110th Cong. (2007); Federal Agency Data Breach Protection Act, S. 1558, 110th Cong. (2007); Federal Agency Data Breach Protection Act, H.R. 2124, 110th Cong. (2007) (similar to S. 1558); Identity Theft Protection Act, S. 1178, 110th Cong. (2007).

tance we place on the subject of private entities making statutory determinations as to whether or not the notification duty is triggered, some brief mention of the parameters of the debate are worth discussing. Even a cursory examination will aptly reveal the potential dangers and conflicts of interest with leaving the "foxes to guard the henhouse." The bills before Congress have provisions similar to those in Senate Bill 239[358] which allow the party who suffered the breach to decide if there is a "significant risk" that the security breach will "harm"[359] the person whose data was taken.

For example, Senate bill introduced by Senator Leahy: the Personal Data Privacy and Security Act of 2007, provides for a "safe harbor" provision that is triggered after:

> [A] risk assessment [done by the agents of the breached entity] concluded that there is no significant risk that the security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach.

A threshold question is, what is a "significant risk" and how is that determination made? How is the bill defining "harm"? Who makes such determination and upon what is it predicated? It is interesting to note, harkening back to the issued covered in the cracked definitional debate that for purposes of defining ID theft, Sen. Leahy's bill incorporates the ID Theft Deterrence Act definition of when ID theft occurs.[360] Recall, this definition labels ID theft as occurring the moment the PII is transferred in an unauthorized manner, by and to someone who has the intent to use the information in an unlawful or wrongful manner.[361]

Therefore, as we read the law, ID theft will occur as a result of many data breaches where intent to commit an illegal or harmful act can be established.[362] Yet, if a private entity determines that there is no "significant risk" that "harm" will result, the notification duty is waived. This is, indeed, placing the decision making process in the hands of private players with a "dog in the fight." Also how would this provision in the Leahy bill square with the holdings in the data breach notification cases, where ID theft (actual injury) is deemed *not to have occurred*, as a result of the breach? We argue it cannot square; the two are mutually

358. S. 239, 110th Cong. (2007), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s239is.txt.pdf.

359. Harm is not defined. *Id.*

360. *Id*. at § 3(b)(1).

361. 18 U.S.C. § 1028(a)(7) (2006) To knowingly transfer or use, "without lawful authority, a means of identification of another person with *the intent to commit*, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law." *Id.*

362. Hacking into a database, in other words, coming solely for the data in question, is one sure way.

exclusive because either the definition in Leahy's bill is rendered meaningless, or ID theft has occurred.

Further examples of how this debate may play out are illustrative as well. Having come to grips with the reality that there are only so many ways to "qualify" risk of ID theft, the Securities and Exchange Commission in their proposed data breach notification requirementsexpounded a novel and unique basis for risk analysis.[363] Here the notification duty would be only be triggered by finding there is: ". . . a significant risk that an individual identified with the information might suffer *substantial* harm or inconvenience. . ." This presents a new trigger in addition to the likelihood of the occurrence of harm; it adds another layer of qualification of degree of harm itself.[364] And similar to the proposed federal law, these determinations are placed with agents of the breached party.

One final and, unappealing, from the consumer's perspective, example of how this textual debate might play out arises from the President's Task Force on ID Theft which recently issued data breach notification guidelines for government agencies that may suffer a data breach.[365] While these guidelines do not apply to private entities (unless, perhaps, government entities are outsourcing data process duties to private subcontractors), they merit some coverage for their authoritative and referential guidance.

The Task Force recommends following factors be considered in the wake of a data breach to help decide whether to notify the public:

- How easy or difficult it would be for an unauthorized person to access the covered information in light of the manner in which the covered information was protected;
- The means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;
- The ability of the agency to mitigate the identity theft; and,
- Evidence that the compromised information is *actually being used* to commit identity theft.[366]

363. 73 Fed. Reg. 13692 (Mar. 13, 2008) (emphasis added).

364. Namely, the "harm" has to be "substantial," given the drafting of the proposed regulations one is left to guess whether the "inconvenience" must be "substantial as well, as we can't ascertain with any certainty whether the qualifier "substantial" applies to "inconvenience" as well.

365. The Task Force was mandated by Exec. Order No. 13,402, 71 Fed. Reg. 27945 (May 10, 2006).

366. Memorandum From the Identity Theft Task Force from Attorney General Alberto R. Gonzales, Chair & Federal Trade Commission Chairman Deborah Platt Majoras, Co-Chair 3 (Sept. 19, 2006), *available at* http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf (as an attachment to Memorandum for the Heads of Departments and Agencies from Clay Johnson, Deputy Director for Management of the Office of Management and Budget) (emphasis added).

The last highlighted bullet point is a novel trigger. It takes the subject out of the traditional "risk based analysis" into an actual requirement that "compromised information" is actually being used to commit identity theft. Again, how is ID theft defined in this Task Force document? Like Senator Leahy's bill, the document cites directly to the definition of ID theft enunciated in the ID Theft Deterrence Act of 1998. Once again, and at the risk of trying the reader's patience, recall this is the definition that requires the "intent" to use the accessed data in question, for an unlawful purpose. This does not, however, prevent the Task Force Authors from misreading the statutory standard, for they later note that:

> Identity theft, a pernicious crime that harms consumers and our economy, occurs when individuals identifying information *is used* without authorization in an attempt to commit fraud or other crimes.[367]

Our main goal in wading into the mire of textual interpretation of proposed statutes, guidelines, and regulations is not to become bogged down in the minutia of data breach notification. Rather, our goal is to try and demonstrate how complex and vitally important the issues are, facing those who will be determining what triggers data breach notification duties, which ultimately will affect hundreds of millions of citizens and determine the nature and scope of IDT.

To be sure these agents of the breached entities face a nontrivial compliance task. ID theft domain experts, after all, have a difficult time establishing a causal relationship between data breaches and the likelihood of any subsequent wrongful use of the identity artifact. Given the time it often takes to manifest the damages from ID theft, someone assessing the causal relationship might have to wait eighteen months or so before they can offer an opinion. Combine reliance on off-the-shelf, plug-and-play software to make determinations on the likelihood individuals whose data has been stolen, with the gutting of state laws that offer the most meaningful protections for these same individuals in question, and we have a recipe for disaster. Yet this appears to be the direction the nation is heading in.

In conclusion, we do not contend every agent of entities confronted with reaching these conclusions will do so in bad faith. It is our contention they will confront these pressing issues with a marked conflict of interest. Importantly, the decisions which corporate entities reach will go a long way to determining how identity is manifest in our society, as well as what digital artifacts will be normalized in establishing a hierarchy of identity attributes. Because of the far-reaching social consequences of these decisions, they must not be ultimately decided behind closed-door boardrooms of relatively unregulated corporate entities.

---

367. *Id.* at 1 (emphasis added).

C. The Market for Identity –Privacy and Security Perceptions Create Reality

Increasingly, unregulated or under-regulated capitalism characterizes the United States economy.[368] Witness the privatization and deregulation of our airline,[369] telecommunications,[370] energy,[371] and financial[372] sectors. While we openly acknowledge that economics analyses are beyond both the scope of this paper and the authors' expertise we note that some dynamics are so pervasive and obvious that the layperson's observation is not to be ignored.[373] As noted in the previous section, this policy of industry self-regulation is patent and growing. Notably, it is not an issue relegated to those with a natural bent to criticize elements of the American capitalist economy. James Cramer of MSNBC *Mad Money* commented in a recent speech:

> Ever since the (President) Reagan era, our nation has been regressing and repealing years and years worth of safety net and equal economic justice in the name of discrediting and dismantling the federal government's missions to help solve our nation's collective domestic woes," he said. "We call it deregulation . . . a covert attempt to eliminate the federal government's domestic responsibilities in regard to on-line privacy protection in the United States.[374]

Cramer went on to note that: ". . .deregulation is the equivalent of saying that "private industry will do it better, that volunteers will do it better, that business if left unfettered will produce so many rich people that they will do it better than the government can."[375]

George Soros, legendary capitalist and albeit frequent critic of the US economy, perhaps put his finger on the key point with regard to overly aggressive deregulation when he said in a recent interview in the

---

368. *See, e.g.,* Bucknell University, *Jim Cramer Challenges 'Laissez Faire' Government,* Jan. 30, 2008, http://www.bucknell.edu/x40027.xml (citing Jim Cramer, remarks at the Bucknell Forum (Jan. 29, 2008)).

369. Airline Deregulation Act, Pub. L. 95-504, 92 Stat. 1705 (1978) (codified at 49 U.S.C. § 1301).

370. Telecommunications Act of 1996, Pub. L. 104-104, 110 Stat. 56 (1996) (codified as 47 U.S.C. § 609).

371. Energy Policy Act of 1992, Pub. L. 102-486, 106 Stat. 2776 (1972) (codified as 42 U.S.C. § 13201).

372. Sarbanes-Oxley Act of 2002, Pub. L. 107-204, 116 Stat. 745 (2002) (codified as 15 U.S.C. § 7201).

373. What separates the expert and non-expert is an understanding the causes and effects of the given subject matter.

374. *See* Jonathan P. Cody, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 Cath. U. L. Rev. 1183 (1999).

375. *Id.*

New York Review of Books:[376]

> So you have to recognize that all of our constructions are imperfect. We have to improve them. But just because something is imperfect, the opposite is not perfect. So because of the failures of socialism, communism, we have come to believe in market fundamentalism, that markets are perfect; everything will be taken care of by markets. [But} markets are not perfect. And this time we have to recognize that, because we are facing a very serious economic disruption.
>
> Now, we should not go back to a very highly regulated economy because the regulators are imperfect. They're only human and what is worse, they are bureaucratic. So you have to find the right kind of balance between allowing the markets to do their work, while recognizing that they are imperfect. You need authorities that keep the market under scrutiny and some degree of control. That's the message that I'm trying to get across.[377]

It was not surprising that this spirit of excessive capitalism and under-regulation would find fertile soil in the digital world, one infamous for its alleged ability to escape jurisdictional boundaries, tax regimes, and regulatory requirements of all governments. Control of resources has shifted away from the public to the private sector and society increasingly relies on the market –whether providing for drinking water in the wake of Hurricane Katrina,[378] or food and drink to our troops in Iraq[379] –to provide and distribute goods and services.[380]

Given the breadth and scope of this shift, it is unsurprising that these "goods and services" now include the intangible forms, i.e. data and personal information, which, when aggregated, make up our digital personas. Society has yet to fully understand the ramifications of outsourcing traditional government functions such as law enforcement, let alone grasping the implications of diving eyes-closed into a regime where identity is no longer being furnished by the government.

In a 1997 paper, *Global Framework for Electronic Commerce,* the Clinton Administration advocated industry self-regulation to protect

376. George Soros & Judy Woodruff, *The Financial Crisis: An Interview with George Soros*, NEW YORK REVIEW OF BOOKS, May 15, 2008, *available at* http://www.nybooks.com/articles/21352.

377. *Id.*

378. Michael Barbaro & Justin Gillis, *Wal-Mart at Forefront of Hurricane Relief*, WASHINGTON POST, Sept. 6, 2005, at D01.

379. Pratap Chatterjee, *Halliburton Makes a Killing on Iraq War*, ALTERNET, Mar. 23, 2003, http://www.alternet.org/story/15445/.

380. For a good description and accounting of how goods and services, once exclusive to the functioning of our democratic government, have been outsourced to the private sector, *see* NAOMI KLEIN, SHOCK DOCTRINE: THE RISE OF DISASTER CAPITALISM (Metropolitan Books 2008).

consumer information online.[381] Furthermore, the nation's foremost authoritative guidance for tackling cyber security, the 2003 *National Strategy to Secure Cyberspace*, explicitly pronounced unwitting trust in the private sector to prevent cybercrime.[382] As discussed, we are certainly witnessing a manifestation of "industry self-regulation" in the unfolding jurisprudence and regulatory regime of data breach notification issues.

In the context of digital identity provisioning, the handwriting is on the wall and being born out. Specifically as related to IDT, it is acknowledged that fraudulent creation and use of identity breeder documents –passport, driver's license, social security card– issued exclusively by the government strikes at the Achilles' heel of identity integrity and is a problem for which the government is failing to resolve.[383] In an effort to address this arguable over-reliance on breeder documents whose vulnerability to fraud is showing no signs of slowing, the market is promoting new ways to authenticate identity such as KBA (knowledge-based authentication), smartcards, and other "strong-auth" type mechanisms.[384] What is happening is that rather than relying on traditional authentication mechanisms issued by the government and over which the market has little control, the unregulated private sector is filling the need for more robust identity reliability and creating an identity regime not based on the context of our physical persons –aka, the digital identity.

It is understandable that putting one's arms around the extent of IDC is problematic in light of how digital identity is being commoditized, a process that feeds on the "scope creeping" of identity documentation. This is strongly illustrated in the case of commercial use of and reliance on the SSN and driver's license ("DL"). The SSN is used by financial institutions, real estate professionals, the healthcare system and other industries as a de facto identifier, despite the fact that it was originally issued by the federal government for the purpose of tracking retirement benefits. Similarly, the DL has become the de facto identification card,

381. Bucknell University, http://www.bucknell.edu/x40027.xml (posted Jan. 30, 2008).

382. *See* President's Critical Infrastructure Prot. Bd., The National Strategy to Secure Cyberspace (2003), *available at* http://www.-whitehouse.gov/pcipb/cyberspace_-strategy.pdf; Brian Krebs, *Cybersecurity Draft Plan Soft on Business, Observers Say,* WASHINGTONPOST, Sept. 19, 2002 (stating that "intense lobbying from the high-tech industry has pulled nearly all the teeth from the plan when it comes to steps the technology industry should take.").

383. As stated in the beginning section on identity and authenticity, our identity is primarily based on the context of our physical beings, our carbon-based life forms. This is the context, therefore, around which we have based our laws and social norms and customs.

384. Strong authorization "is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network." Strong Authentication at Fermilab, http://www.fnal.gov/docs/strongauth/ (last visited Nov. 21, 2008). *See also* RSA Information Security Glossary, *strong authentication*, http://www.rsa.com/glossary/default.asp?id=1080, (last visited Nov. 21, 2008.

yet it was issued by state motor vehicle agencies for the purpose of enhancing public roadway safety.

The repurposing of identity artifacts for commercial use took a profound evolutionary leap with the aid of other environment variables. For instance, business uptake of technology advances in capture, storage, transmission and analyses of this data provided unprecedented abilities to migrate business processes into the information age. In order to monetize these newly migrated or generated products, user registration became a prerequisite. This has further evolved the creation of more products and services, further exchange and disclosure of personal information, and an incentive to invent new forms of consumer profiling and targeting to not only sell those products, but to stimulate advertising revenue. A seminal illustration of this cycle is the eruption and ubiquity of ad space on websites.[385]

The sprouting of online behavioral target marketing further exemplifies the drive to leverage technology advancement (storage, communications, and analysis) to overcome physical world, time-space constraints and narrow the gap between business (supply) and customer (demand). A consequential effect is that identity is being exploited via commoditization in order to narrow the gap between business-supply and customer-demand.

A compelling case study for the increasing command of the private sector over PII is the prosperity and proliferation of the search engine business model, which owes it prominence if not existence to online targeted, and behavioral advertising, and which has spawned an entire field of marketing strategy.[386] The poster child for this truth is none other than Google, which has transformed itself from an engineering company valued for its information retrieval technology into an advertising and marketing company. Similarly, the skyrocketing valuation and proposition for cyber social networks illustrates the hunger to capture our digital personas.[387] PII is fueling this engine. It is both the content and commodity, which the market wants to control in order to maximize

385. *See* PRIVACY INT'L, A RACE TO THE BOTTOM: PRIVACY RANKING OF INTERNET SERVICE COMPANIES, A CONSULTATION REPORT (2007), *available at* http://www.privacyinternational.org/issues/internet/interimrankings.pdf.

386. SEO, or search engine optimization, is a marketing strategy for increasing a site's relevance, SEO considers how search algorithms work and what people search for. SEO efforts may involve a site's coding, presentation, and structure, as well as fixing problems that could prevent search engine indexing programs from fully spidering a site. Other, more noticeable efforts may include adding unique content to a site, ensuring that content is easily indexed by search engine robots, and making the site more appealing to users. *See, e.g.,* Wikipedia, *Search Engine Optimization,* http://en.wikipedia.org/wiki/Search_engine_optimization (as of Sept. 2, 2008).

387. *See, e.g.,* Catherine Holahan, *Google's DoubleClick Strategic Move*, BUSINESSWEEK, Apr. 14, 2007, http://www.businessweek.com/technology/content/apr2007/tc20070414_675

profits in the spirit of laissez faire capitalism.[388]

A full decade ago, legal academician Jerry Kang reflected on this free market commerce argument which holds, for example, that that personal information flows will decrease transactions costs by helping creditors avoid bad risks and minimize associated premium costs for consumers; decrease search costs between buyers and sellers; and, enhance the quality of direct marketing to individuals. He commented that he: "believe[s] that such practices violate the users' rights to "information privacy," which is defined as the right of an individual to control the acquisition, disclosure, and use of personal information. Site operators argue that the collected information is a valuable commodity, and that they have the right to exploit it commercially. This argument is strengthened by the fact that the "postindustrial economy generally and the telecommunications sectors particularly are seeing increased competition . . . [prompting] firms to exploit every competitive advantage, including the use of personal information."[389] To the extent this observation was true when the Internet and e-commerce was in its preemie stage, what is occurring now is orders of magnitude greater.

The protection and maintenance of an authentic digital persona via digital security is central to countering electronic crime and promoting consumer faith in the marketplace. Primarily to date, this has been left to the market forces, which concomitantly promotes the unregulated and unobstructed, flow of highly personal information. This flow is predicated on easy credit, which in turn fuels the consumer economy. The market forces favor efficient, friction-free environments, where one of the ultimate goals is to maximize benefits and reduce cost for the respective corporate shareholders. A collateral effect and negative externality has been an explosion of data breaches and ID theft resulting from such activities.[390] The rising fraud costs from ID theft, account hijacking, data leakage, and phishing in the face of the ever-growing list of competing products and standards is a clear sign that the market is failing in the security realm perhaps at the expense of the free flow of PII. Courts, legislation, and regulation are often perceived as standing in the way of the market's "goals."

511.htm?campaign_id=rss_daily; *Google Buys Facebook,* INFOWORLD, Apr. 1, 2008, http://www.infoworld.com/article/08/04/01/14FE-april-fool-google-facebook_1.html.

388. William J. Frawley, Gregory Piatetsky-Shapiro & Christopher J. Matheus, *Knowledge Discovery in Data-bases: An Overview,* 13 AI MAGAZINE 58 (1992), *available at* http://www.aaai.org/ojs/index.php/aimagazine/article/viewArticle/1011.

389. *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1238 (1998).

390. Whatever confusion about the actual numbers of people affected by ID theft or cybercrime in general, scant few argue that the numbers, in both people affected and resulting damages, are insignificant.

In addition to the consumer and market-driven information economy just discussed, these two additional dynamics are reflective of free market policy drivers,[391] which exert profound and omnipresent, yet hard to measure and counteractive pressure on privacy and digital security policies. Any combination of these dynamics that affect privacy and digital security policies, impacts cybercrime and specifically, ID theft. To the extent there is an ID theft crisis, its existence cannot be divorced from the following dynamics outlined in the next few paragraphs. All of these various interests are impacted by policy derived from legislatures and courts, as expressed in laws, regulations, and administrative and judicial decisions, or lack thereof. In some instances the "impact" is even designed.

First, this consumer and service-oriented American economy is fueled by cheap labor, the practical reality of which often involves illegal or quasi-legal labor. These laborers must have some identifying documentation that is capable of satisfying employment requirements governing businesses to ensure compliance with employment laws. In short, employers of cheap labor and the workers themselves are highly motivated to secure proper identity documentation and impersonating a qualified identity is often the only way for that to occur.[392]

Second, information service providers and content owners are capitalizing on the value of intellectual property in this information economy, and are thus proliferating and building a strong lobby to monetize their intellectual property ("IP") rights. These service providers and IP owners have a powerful incentive to track, harvest, and protect their intangible assets, which often entails contravening privacy and security interests and controls that individuals and entities have in their data and systems.

Lastly, the American national security environment, undoubtedly driven by unprecedented international terrorist events and corporate espionage, is fervently driven by the need to protect the nation and its assets from the new threat and face of terrorism. The ISE, Information Sharing Environment, is an entire federal office within the national intelligence directorate that was formed after the 9/11 terrorist attacks on New York and the Pentagon, partially in response to criticism that a lack of information sharing among the government agencies was a reason

391. The authors acknowledge there are other dynamics that effect privacy and digital security issues. Most specifically, we refer to consumer interest groups. But compared to the free market forces we see, their influence as tepid, and erratic, at best.

392. *See* Bianca Vazquez Toness, *Raid on Illegal Immigrants Brings Chaos to Town*, Mar. 14, 2007, *available at* http://www.npr.org/templates/story/story.php?storyId=8904390; Nuclear Rays from My Halogen Haze, http://nuclearraysfrommyhalogenhaze.wordpress.com/2008/08/27/600-detained-in-mississippi-plant-raid-suspected-of-being-illegal-immigrants/ (last visited 16 October 2008).

that those events were not prevented. Significant human and economic resources continue to be expended to monitor and disseminate communications, transactions, and movements of persons suspected of posing a threat to our nation and to the world.[393]

IV. THE ROLE OF LAW ENFORCEMENT AND IDC

One of the central premises of this paper is that given IDC data deficiencies, we have no baseline understanding of the nature and scope of the problem. Any entity, whether it is LE or corporations in any industry, uses benchmarking to understand risk and the effectiveness of responses. In other words, baselines and benchmarks define the results. When no baseline of data is established, no benchmark exists, and decisions are indubitably made on partial data.

The social institution, which has traditionally stewarded this baseline knowledge of social wrongs because it is uniquely positioned to collect ground truth data on lawbreaking, has been law enforcement, and more specifically, local law enforcement. Regarding the three-ring circus of IDC, LE has assumed the role of spectator as a hybrid result of the aforementioned policy-backed lack of security accountability, and LE has been willing to cede IDC as a self-correcting problem for the market to solve. This is particularly significant because it is a self-reinforcing black hole: unlike traditional crime, LE is no longer the frontline interface for corporate or citizen-victim reporting.[394] Individuals are apathetic about LE's earnestness in taking and investigating reports, reporting that does occur is handled privately, civilly or via regulatory action, and this results in a dearth of aggregate, objective data on the nature and extent of the problem.[395] In turn, LE and the aggregate public it serves are on the short end of IDC threat information asymmetries, which then cripples the accurate allocation of resources for LE to get into the game, thereby reinforcing LE as a spectator to the problem.[396]

---

393. *See, e.g.,* Carl Hulse & Edmund L. Andrews, *House Approves Changes to Surveillance Program,* INT'L HERALD TRIBUNE, Aug. 5, 2007, *available at* http://www.iht.com/articles/2007/08/05/america/spy.php; K.C. Jones, *White House Wants Immunity for Electronic Surveillance,* INFO. WEEK, Jan. 24, 2008, *available at* http://www.informationweek.com/news/management/showArticle.jhtml?articleID=205918006; Siobhan Gorman, *NSA's Domestic Spying Grows as Agency Sweeps up Data*, WALL STREET J., Mar. 10, 2008, http://online.wsj.com/public/article_print/SB120511973377523845.html.

394. With the exception of recent breach notification laws corporations have very little incentive to report IDC to LE and in fact may be disincentivized.

395. Victims bear a maximum $50 loss and are generally made financially whole by financial institutions for credit card fraud.

396. *See* Susan W. Brenner, *Toward A Criminal Law for Cyberspace: A New Model of Law Enforcement?*, 30 RUTGERS COMPUTER & TECH. L. J. ___ (2003), *available at* http://pegasus.rutgers.edu/~rctlj/; UNITED NATIONS INTERREGIONAL CRIME & JUSTICE RESEARCH

A. Twenty-First Century Law Enforcement: Priced Out of the IDC Market

Both corporate America and the government are concerned about consumers losing faith in the marketplace. One issue that has engendered scant attention in public debate is the harm from loss of faith in the law and law enforcement. Legislative and judicial decision makers have honed their radars on the direct costs to citizen-victims and the economy. This myopia ignores the more insidious downstream and implicit costs of IDC.

We must reassess the notion of harm in order to evaluate the aggregate, negative social impact of IDC. The ripple effect of an incident may go far beyond the reported damages and loss currently defined in prosecutorial policy and civil liability. Anecdotal data and other available indicators reveal variable rates and costs of IDC, but that data is only a small subset of the actual prevalence of IDC. Measuring the social impact and derivative effects on critical infrastructure using a financial impact model is turning a blind eye to the reality of insidious harm that flows from identity pollution. Market-dominant responses to IDC perpetuate the private policing of a problem, which demands solutions at a level beyond the individual balance sheet and corporate shareholders and fund managers. The under-representation of LE in addressing IDC is a major contributor to our current state of ignorance as reflected in the lack of metrics, as well as the resulting ineffective prevention and reduction strategies to lower the IDC risk. LE needs to resume its place as a critical trusted intermediary, of crime statistics particularly, in the flow of IDC information.[397]

Why is it that a victim of a robbery would not hesitate to turn to LE, yet has nearly the opposite response when his identity is thieved and abused? What does the gross discrepancy between hundreds of millions of compromised identities from data breaches, the estimated billions of dollars lost to this fraud, and the miniscule number of valid LE incident reports and criminal prosecutions mean? There is little attribution, or closing the loops between criminal threats, data vulnerabilities and loss events. As corporate victims brush costs under the rug and/or deploy private, or even industry-wide counterstrategies, the cost of IDC just gets shifted with little deterrent effect on the underlying problem. If we analogize the response to IDC as a four-legged stool with victim advo-

---

Institute, The Challenges of Cybercrime, 2002 Journal 14, http://www.unicri.it/news/UNICRI%20Journal%202002_1%20FINAL.doc.

397. *See* United States General Accounting Office, Identity Theft: Greater Awareness and Use of Existing Data Are Needed, GAO-02-766 17-18 (2002) (finding that law enforcement agencies have insufficient resources to investigate and prosecute and that identity theft cases often end without an arrest).

cacy, legislative and judicial policy, and corporate security as three of the pillars, there is grossly disproportionate attention paid to the LE leg. Society assumes that the traditional business model of LE, comprised of the people, processes and technology to respond to and enforce traditional analog crimes like burglary and assault, is the same model that can effectively address identity crime. This assumption quickly breaks down as citizen-victims are forced beyond the current apathetic and discretionary reporting dynamic.

Society is harboring under gross misperceptions that LE is situated to effectively handle the current and oncoming deluge of IDC reports. LE is failing as a "frontline manifestation of society's determination to establish a reliable digital environment." One end of the spectrum has local LE posturing that the problems are too unbounded and multi-jurisdictional; while federal LE bemoan that the ground level issues are too nickel-and-dime to warrant their attention. Both perspectives are fueled by a poor infrastructure to act upon both the relatively small numbers of officially reported cases, not to mention the treasure trove of IDT complaint reports that are not validated. If ever there was a crime that necessitates cross-jurisdictional sharing and linking of reports, IDT certainly sits in pole position.

LE's current infrastructure for collecting, investigating and prosecuting IDT is largely steeped in the physics of traditional crime, which is to say that information is not aggregated or matched across jurisdictional record-keeping but rather is compartmentalized in and dispersed within agency information silos. This contributes to the well-earned badge that IDT is a low risk-high reward venture, as criminals exploit the knowledge black holes within the current business model of LE. The dynamics of the discovery, perpetration, and manifestation of IDT means that the rule rather than exception is a minimum of four jurisdictional touch points: (1) the jurisdiction where the theft occurred; (2) where the stolen identity was used; (3) where the victim resides; and, (4) where the suspect originates. A resulting question is: Is society grappling with is whether we are on our own to protect our identities in this information society? We have arrived at this state due to several major deficiencies anchored around reporting and data sharing –the boundary conditions (the policies and procedures instructing the design and application of technologies) which define LE's operating behavior.

Internally, law enforcement is ill equipped to receive and act upon IDC incident reports from victims, especially on the individual rather than the business enterprise level. Reporting is clumsy and ineffective at three levels: at the interface between the victim and LE; internally within the initial collector agencies; and, collectively between LE agencies and across stakeholder organizations nationally. The widespread disagreement about the statistics surrounding ID Theft is diametrically

opposite when it comes to acknowledging reporting deficiencies. This is both a logical and expected validation of the numbers problem discussed previously.Besides the policy disincentives to report the crimes to LE, real and fictional justifications exacerbate the problem.[398] One of the bona fide reasons that seventy-two percent of victims do not feel the need to report is grounded in the mechanics of the reporting process –it is confusing, inconsistent and inefficient.[399]

Some jurisdictions do not take IDT reports, many will take it out of courtesy but with no real follow-through, some will pass off citizen-victims to consumer advocacy-chartered organizations, and those accepting reports use agency-specific, generic crime formats. There is no nationally accepted standard for IDC reports, both at the human-readable and machine levels.[400] This artifact of the traditional model of individual jurisdictional sovereignty is problematic because it assumes a compartmentalized solution to a multijurisdictional, multidimensional, cross-crime problem. If each agency captures IDT-agnostic information in its own format, there is no way to match, link, analyze or compare reports from one agency to another on any level of efficiency.

The result is duplication of reporting and investigation across agencies, an inability to compare apples to apples for information sharing and statistical reporting purposes, and reliance on manual, dumb luck to discover crime information commonalities. It is no wonder that the two-way street of apathy between LE and citizen-victims is a well-paved road. There are reasons why IDT is a high opportunity, low risk crime.[401] IDC and its manifestations are proliferating beyond the time

398. Some common assumptions and myths regarding law enforcement's handling of cybercrime in general and IDT in particular include: destruction of public confidence in the reporting company, negative publicity in general, loss of control, lack of confidence in LE technical and management capabilities, possible competitive disadvantages. *See* Erin Kenneally, *Workshop on Cyber Crime Reporting: Challenges and Issues, Proceedings Report and Recommendations*, San Diego Supercomputer Center University of California San Diego (Jan. 13, 2004).

399. FEDERAL TRADE COMMISSION, 2006 IDENTITY THEFT SURVEY REPORT (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

400. The President's Taskforce on Identity Theft and IACP Resolution recommends a uniform IDT crime report.

401. These technological innovations have forever changed the way ordinary people do business and clearly have positive aspects. The new technological revolution, however, also has a down side. The increased accessibility to personal information has provided identity thieves with new opportunities to engage in criminal activity. This technological change may be viewed in terms of routine activities theory, which states that when the three elements of offenders, victims, and lack of capable guardianship meet in space and time, crime is likely to occur. It is reasonable to propose that advances in technology have altered two of the three elements in this theory, specifically victims and guardianship. With regard to victims, there may be a greater abundance of suitable targets due to greater amounts of accessible, personal information being stored on the Internet than ever before. With re-

and space boundaries that the LE business model is built upon, and those legacy reporting dynamics and management are pressured well beyond resource capacity and scale.

The IDC reporting that is more consistent, comprehensible, and structured is predominantly generated by the FTC or Internet Crime & Complaint Center ("IC3"). The problem which all too many are unaware is that those "reports" are not validated by any authority let alone LE, and consequently there is no requirement that LE take action upon or disposition of these complaints. Only 2,100 of the more than 17,000 law enforcement agencies in the United States accept complaints from the IC3. And only a fraction of total LE agencies interact with the reports store-housed by the FTC in its Consumer Sentinel database.

Another reason for the state of cardiac arrest in IDC reporting, exacerbated by the formatting and disposition dynamics, is that the recorded data are not migrated over to Uniform Crime Reporting ("UCR") and National Incident-Based Reporting System ("NIBRS"), the crime reporting standards responsible for national benchmarking and baselining of all crimes. The FTC and IC3 complaints are never ingested into LE crime and incident databases so they are not reflected in national criminal stats. IDC reports collected by LE are retrofitted into traditional, broad crime categories such as general "theft." UCR and NIBRS offense codes available for law enforcement reporting do not differentiate Identity Theft crimes (or cyber or computer crime for that matter) from the more traditional fraud and larceny offenses. This serious oversight in our national crime reporting standards forces law enforcement agencies to retrofit IDC as fraud, larceny, or impersonation.[402] When IDC cases are embedded in these traditional reporting statistics the result is a seriously skewed statistical analysis for identity and all crime types, and an exacerbation of definitional confusion.

One final aspect of the reporting problem is that IDC information is often not standalone even though it is treated as such. These crimes commonly overlap with and/or are breeders for traditional crimes such as

---

spect to guardianship, this element may have been reduced because of insufficient regulations formally protecting against personal information being abused. These changes to the elements of victims and guardianship from technological advances may have had the effect of increasing the number of identity theft incidents. *See, e.g.*, Stuart F. H. Allison, Amie M. Schuck, & Kim Michelle Lersch, *Exploring the Crime of Identity Theft: Prevalence, Clearance Rates, and Victim/offender Characteristics* 33 J. CRIM. JUSTICE (2005) 19.

402. For instance, the top frequent crime types used to charge IDT in San Diego County were BURGLARY, FRAUD, FORGERY, THEFT, DRUG-RELATED OFFENSES, VEHICLE THEFT, EMBEZZLEMENT, DUI, ASSAULT, and WEAPONS OFFENSES. Julie Wartell, *Geography of Identity Theft: Analysis of San Diego County Data*, July 2008. Furthermore, IDT has in the past been charged under any of the approximate 66 related penal code charges in California (analyzed as part of the NIJ Project WHO? Identity Theft project, *infra* note 389).

robbery, mugging, pick-pocketing, theft from cars, and burglary. Often the crime incident reporting processes and systems currently used by LE do not have sufficient flexibility to collect the multidimensional criminal acts and information. In addition to the inaccurate recording within the LE justice system, many IDC are similarly not prosecuted or prosecutable as such, again creating barriers to cognitive understanding of the nature and scope of IDC.

Related to reporting deficiencies, the other major boundary condition impeding LE's management of IDC is the systems involved in data sharing. The information systems do not allow investigators and analysts to check across different crime incidents and IDC reports to uncover overt similarities between cases, let alone latent patterns or relationships that speak to underlying problems beyond just cases.

ID Theft spans jurisdictional boundaries: it is not uncommon for the victim to live in one LE jurisdiction, the suspect in another, the identity stolen in a third jurisdiction, and finally, the identity used fraudulently in a fourth. And to complicate jigsaw puzzle, these are usually not discrete events, but rather, episodic and recurring in likely another patchwork of physical and virtual geospaces. LE systems of records are for the most part standalone and not interconnected. LE is relying on manual processes to assimilate and synthesize across ever-expanding data related to IDC incidents.[403]

Continued attempts to manually manage time-intensive knowledge tasks, which are apt for automation, create inefficiencies in resource deployment. This has contributed to a crisis of prioritization where LE does not even know which haystack to start to parse through, let alone begin to find the needles and connecting threads buried within. Workable cases fall through the cracks because of failure to meet jurisdictional and threshold investigation requirements. Investigations are duplicated between agencies because they are operating on incomplete and uncorrelated pieces of the overall crime picture. Thus, the collection, sharing and coordination of IDC data do not scale qualitatively or quantitatively with the IDC threat. Criminals' exploitation of this disjoint is what contributes to the low risk-high reward attractiveness of this crime.

B. Countering Inertia

Despite the reporting and coordination deficiencies, which have created the IDC responsibility crisis, there are definable, measurable and practicable solutions, and innovative efforts to catalyze the necessary

403. For example, in lieu of electronically memorialized and searchable reports, investigators reviewing reports often rely on memory triggers that two or more reports/cases are connected based on common data elements between them.

changes in the currently crippled system.[404] We need to create economies of scale for LE to detect and respond to IDC. These measures are aimed directly at changing the boundary conditions that constrain LE's role in lowering the IDC risk. For one, LE must have a framework for centralized and searchable reporting coordination capabilities related to IDC. Specifically, this entails the ability to digitally collect, communicate, link and analyze data related to suspects, victims and incidents in standard formats.[405]

The substance and mechanics of this standardized reporting should facilitate actionable information exchange. For instance, Web-based reporting of information that is reflective of the supply held by victims and the demands of LE investigation can provide the standardization, convenience, consistency, completeness and accuracy that presently inhibit current cooperation between citizen-victims and LE. Underlying policies and procedures so that the data is meaningful and supportive of counter IDC strategies and enforcement of criminal laws must support this framework.

This framework, enabled by policy and procedure, should be relied upon as a key empirical source of ground truth, and the data generated should be shared with key stakeholders to enable pragmatic prevention, detection and response solutions. As recounted throughout this paper, decision makers are operating from anecdotal and incomplete information about the scope and breadth of ID theft crime. Unless validated first-source data flows into policy dialogues, the executive, judicial, and legislative decision makers will develop and deploy strategies that allocate resources inefficiently and ineffectively. Another aspect of this reliance includes turning to LE as an intermediary, particularly as it pertains to data breach notification incidents that enable the proper transfer of information between citizen-victims and the institutions

404. One such innovative effort is Project WHO? –A Law Enforcement Centric Framework for Managing Identity Theft, funded by the U.S. Department of Justice, National Institute of Justice. The Project WHO? model offers the promise of significant progress toward solving the lack of metrics and detachment problems in ID theft by providing a model technology and policy framework for managing IDC based upon repeatable and familiar processes.

405. The standardization should occur both semantically and syntactically on both the human readable level (i.e, similar data fields across incident and investigation reports) and machine level (i.e, the underlying data model and/or exchange schema such as Global Justice xML ("GJXML") ID Theft Reference Data Model Schema. The aforementioned Project WHO? has developed such a referential IDT schema grounded in GJXML. *See also* The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ()Apr. 2007), *available at* http://www.ftc.gov/opa/2007/04/idtheft.shtm.

stewarding identity artifacts.[406]

Finally, this reliance on LE as an empirical source of metrics demands appropriate funding resources. The commitment by LE must be matched by a financial commitment from society. Otherwise, we have created an unfunded mandate whose failure is imminent.

The market and its servant technology should assume the lead with regard to various solutions aimed at protecting, authenticating and validating identity. However, it cannot reign supreme –society must have a role in the decision making process. This involvement introduces friction that impedes market dynamics. Our perspectives must shift to viewing the role of society –as represented by LE and public institutions, as a necessary source of "Q & A" that can validate market efforts in IDC. We need to engage in basic questions such as: What are the policies driving attempted solutions to the problem and why are we implementing them in the manners chosen? What are the benefits and dangers? How do we avoid the latter? Perhaps society is willing subsidize IDT losses, but no one is asking and society is not being given a seat at the table in making the economic decisions and asking how we arrive at those numbers. Local LE has a pivotal yet underrated and unrealized role in this Q&A process. It can help manifest what is working by collecting ground truth and assuming its rightful role as trusted intermediary of identity vulnerabilities.

V. CONCLUSION

This paper developed the following proposition, albeit raising as many questions as it attempted to answer, with the objective of raising the level of discourse surrounding identity crime:

1. ID crime in the U.S. is a cascading effect of the culmination of public policy (i.e., law, regulation, jurisprudence) decisions or non-decisions. The present policy regime incentivizes information availability and use. These policies define and shape our current free market socioeconomics by facilitating a relatively unrestricted flow and mining[407] of a commodity: data that includes personally-identifiable infor-

406. *See, e.g.,* CAL. CIV. CODE § 1798.82. For example, the California data breach notification law provides an exception that allows delaying notifcation for "the legitimate needs of law enforcement." *Id.*

407. We use the term to encompass more than the other techniques such as statistics, OLAP, data warehousing, but rather, "the nontrivial extraction of implicit, previously unknown and potential useful information from data." Frawley et al., *supra* note 389. *See also* Jesus Mena, *Data Mining FAQs,* DM REVIEW (1998), *available at* http://www.dmreview.com/master.cfm?NavID=198&EdID=792. Data mining differs from other data analysis methods in several different ways, significantly, in who and how the query is performed. See, in data mining, the interrogation of the data is done by the machine-learning algorithm or neural network, rather than by the statistician or business analyst. Tradition-

mation. The notion that "information is a commodity," in and of itself has matured to the point of being a cliché.

2. This dynamic, taken to its logical conclusion, means that the market demands the uncontrolled and frictionless flow and mining of personal information in order to fuel the credit and sales (including advertising and marketing services) channels upon which our economy is grounded. IDC is an externality, the collateral damage if you will, of free market domination of the digital persona.

3. These values embedded in socioeconomic policies conflict with a coexistent socioeconomic policy which demands greater data security and privacy controls that promote prevention, detection and response to personal data insecurity. Near complete domination by the former necessarily means that security and privacy vulnerabilities persist in order to enable that free flow and manipulation mining of information.

4. Implicit in this policy, which incentivizes free flow of data, is a corresponding poor allocation of incentives to secure data. One consequence is personal data vulnerability, including failure to disclose vulnerabilities. Knowledge about the vulnerabilities puts people on notice. It imposes management costs, which introduce friction because it allows the assignment of responsibility and imposition of duty for personal information security controls.

5. The social institution, which has traditionally been best, situated to steward this knowledge of social wrongs via collection and dissemination of aggregate statistics and analyses has been law enforcement. Given the policy-driven lack of security-privacy accountability, there is little to enforce and even less objective information upon which to understand the problem and allocate resources accordingly. In the end, local LE's speculative role is augmented by secondary, anecdotal information, with questionable reliability. For the legal boundaries that do exist, enforcement is handled civilly or regulatory, resulting in threat information asymmetries for LE and the public it serves.

6. The result is a knowledge gap and misunderstanding of the nature and extent of this information corruption and misuse. Therefore, the nature of the threat is masked and policy is informed by incomplete, in-

---

ally, the goal of identifying and utilizing information hidden in data has been achieved through the use of query generators and data interpretation systems such as SPSS or SAS, the traditional tools of database analysis. These statistical methods require the user to format a theory about a possible relation in a database and to convert the hypotheses into a query. It is a manual, user-driven, top-down approach to data analysis. In contrast, in data mining, the interrogation of the data is done by the data mining algorithm rather by the user. The uniquely dynamic feature of data mining allows the analyst to mine the data without pre-prepared questions or problems to resolve. Data mining uses discovery-based approach, meaning that it discovers hidden structures, ratios, patterns, and signatures to determine the key relationships in the data.

accurate, and self-serving or biased versions of the "truth." The lack of standard definitions, objective statistics and empirical tracking of IDC leaves little for the legislature and judiciary to inform their solutions. What results is a breeding ground for privatized solutions and self-perpetuating, vicious cycle.

It is certainly not in the best interests of the free market to accurately report this gap. These security-privacy vulnerabilities have incentivized the exploitation of personal information. Witness the black market/underground economy and aboveground criminal use of identity data. This has negatively affected the authenticity and reliability of our digital identities, which in turn has contributed to the chaotic digital environment.

7. Unless technology policy shifts to create a better equilibrium between the need for security-privacy enforcement and the free market agenda, corrupted digital personae may pervade the landscape. If digital identity is defined by market-driven policy, individuals will be left to the tender mercies of the various marketing and legal departments with the presumption that they negotiate privacy protection with those market entities (i.e., vendors, merchants, creditors) on their own. Will consumers enter into meaningful agreements with these entities to disclose PII breaches or misuses? This opens the door to the creation of classes of privacy divided on socioeconomic lines, among others. If privacy is a civil liberty right akin to free speech, it should not be commoditized as something that can be bought and sold. If it is treated as such, what we risk is information asymmetries, where citizen consumers are left without knowledge of their privacy vulnerabilities or rights to remediation. Relegating detection and protection of fundamental privacy rights to case-by-case determinations is both inefficient for citizen consumers and it fails to provide the deterrent effect that influences both normative and deviant behavior.

Digital identity may be defined or corrupted by the entities promoting the capitalistic bottom line, which heretofore has treated identity as an alienable commodity that demands an unrestricted flow in order to maximize profits. Its proponents would argue that if such treatment fails to promote the "bottom line" and the balance tips in favor of greater privacy protection over free flow, the market will self-correct to give consumers what they demand. However, this ignores the intangible costs, which we have yet to quantify on the balance sheets: widespread and aggregate indeterminism of identity reliability and reputation pollution. This cost goes beyond financially remediating IDC victims for out-of-pocket losses and underwriting fraud losses as a cost of doing business, but rather, includes the pollution of any activity that is predicated on the authenticity of the person behind the transaction. If an economy predicated on knowing the intrinsic value of identity is no longer able to, we

have fertile breeding grounds for Grand Canyon gaps between perception and reality. In order to prevent participants in this economy from jumping ship, one probable solution is to create false illusions of reliability and control over one's digital integrity.