Notre Dame Journal of Law, Ethics & Public Policy

Volume 28
Issue 2 *Symposium: White Collar Crime: The Moral, Ethical, & Legal Implications of White Collar Crime in the 21st Century*

Article 3

6-1-2014

White Collar Crime: What It Is and Where It's Going

Gerald Cliff

Christian Desilets

WHITE COLLAR CRIME: WHAT IT IS AND WHERE IT'S GOING†

GERALD CLIFF* & CHRISTIAN DESILETS**

We present this work to help clarify the concept of white collar crime, discuss what it has traditionally been perceived to be and what it is becoming in the age of computers, the Internet, and rapidly advancing technology. In the end, the reader will hopefully have a better understanding of the nature of white collar crime, its impact on our society and the direction in which it seems to be heading.

We begin with a brief discussion of the term "white collar crime," first coined in 1939 by Edwin Sutherland, and further explored, refined, and redefined by a number of successors in various fields. We examine various definitions, as well as the reasons why so many different definitions exist, and discuss both efforts to unify these definitions and to work with terminology that means different things to different criminal justice stakeholders.

We then move on to discussing the general shape of white collar crime in America, the relevant data for various types of activities that meet the criteria for at least some of the most prevalent white collar crime definitions, and how to interpret that data.

Finally, we examine two areas of emerging concern in the field of white collar crime—social media and privacy.

---

† This Article was produced as part of the research and work of the National White Collar Crime Center (NW3C). The mission of the NW3C is to provide training, investigative support, and research to agencies and entities involved in the prevention, investigation, and prosecution of economic and high-tech crime.

This project was supported by Grant No. 2012-BE-BX-K002 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

* Research Director, National White Collar Crime Center. Ph.D., Wayne State University.

** Research Attorney, National White Collar Crime Center. J.D., Georgetown University Law Center.

I. DEFINITIONS OF WHITE COLLAR CRIME

A. *Multiple Definitions*

The term "white collar crime" means different things to different disciplines, as well as to different camps within those disciplines. Unfortunately, professionals within an environment where there is general consensus about the term's meaning do not always clearly specify what they mean by the label of "white collar crime." This can lead to confusion and (sometimes vigorous) disagreement when they interact with larger audiences that might contain a number of different understandings of the term. It is therefore quite important, when discussing white collar crime, to more closely examine what different people mean by it. Generally, these definitions tend to concentrate on: the characteristics of the offender (such as high social status) and/or the characteristics of the crime (such as crimes occurring within the scope of one's employment).

In the late nineteenth and early twentieth centuries, the theoretical constructs used by sociologists to understand crime focused on it as a problem of poverty and of personal characteristics believed to be associated with poverty (such as broken homes, mental illness, association with criminal subcultures, and living in slum housing). One of the most influential of those theories, Anomie Theory, is still in general use (in various forms) today, and was put forth a year before the introduction of the concept of white collar crime.[1] It holds that in a society where members are taught to value attaining certain goals (such as wealth), but the means to achieve those goals are unevenly distributed, those without access to the societally prescribed means are put under considerable pressure to find other ways (including crime) to achieve those goals. In short, the theory holds that crime is a symptom of some members of society not having the tools to achieve what their society defines as success.

The sociologist Edwin Sutherland coined the term "white collar crime" in a speech given to the American Sociological Society in 1939.[2]

1. Robert K. Merton, *Social Structure and Anomie*, 3 AM. SOCIOLOGICAL REV. 672 (1938), *available at* http://www.jstor.org/discover/10.2307/2084686?uid=3739968&uid=2133&uid=2&uid=70& uid=4&uid=3739256&sid=21102625935857.

2. Edwin H. Sutherland, *White-Collar Criminality*, 5 AM. SOC. REV. 1 (1940) (which is the paper version of the Presidential Address of the American Economic Society delivered at Philadelphia, PA, on December 27, 1939), *available at* http://www.asanet.org/images/asa/docs/pdf/1939%20Presidential%20Address%20(Edwin%20Sutherland).pdf.

While he gave no formal definition of the term in the speech, he would eventually define white collar crimes as "crimes committed by a person of respectability and high social status in the course of his occupation."[3] This offender-based (and crime-based) definition was well-suited to the tasks to which it was put, serving to give sociologists a way to label and talk about offenses committed by successful, healthy people who had ample access to societal resources and who were members of respectable society—a concept that was out of synch with the prominent sociological theories of the day. Sutherland's contribution expanded the discussion to include illegal deviance perpetrated by those who had the tools to achieve the goals that their society taught them to desire, and had, in fact, already used them to that effect.

One notable aspect of Sutherland's conception of white collar crime is that he explicitly rejected the notion that a criminal conviction was required in order to qualify.[4] Sutherland saw four main factors at play here: 1) civil agencies often handle corporate malfeasance that could have been charged as fraud in a criminal court, 2) private citizens are often more interested in receiving civil damages than seeing criminal punishments imposed, 3) white collar criminals are disproportionately able to escape prosecution "because of the class bias of the courts and the power of their class to influence the implementation and administration of the law,"[5] and 4) white collar prosecutions typically stop at one guilty party and ignore the many accessories to the crime (such as when a judge is convicted of accepting bribes and the parties paying the bribes are not prosecuted).

A related concept that again focuses on the offender is "organizational crime"—the idea that white collar crime can consist of "illegal acts of omission or commission of an individual or a group of individuals in a legitimate formal organization in accordance with the operative goals of the organization, which have a serious physical or economic impact on employees, consumers or the general public."[6]

While these definitions were vital for expanding the realm of sociology and criminology, they were not as well-suited to the needs of other criminal justice stakeholders who dealt with these issues in a more practical sense (including policymakers, law enforcement, and the legal community). These definitions are geared for asking why white collar crime occurs or who commits it, but they are not as well-suited to asking questions about how much white collar crime is occurring, or whether prevention methods are working.

A model of white collar crime that leant itself somewhat more to empirical data analysis was Herbert Edelhertz's 1970 definition: "An illegal act or series of illegal acts committed by nonphysical means and by concealment or guile, to obtain money or property, to avoid the pay-

3. Edwin H. Sutherland, White Collar Crime: The Uncut Version (1983) (the censored first edition came out in 1949).

4. Sutherland, *supra* note 2, at 6.

5. *Id.* at 7.

6. Laura Shill Schrager & James F. Short, *Toward a Sociology of Organizational Crime*, 25 Social Problems 407, 411–12 (1978).

ment or loss of money or property, or to obtain business or personal advantage."[7] As a crime-based definition, it ignored offender characteristics and concentrated instead on how the crime was carried out. As a result, it covered a far larger swathe of criminality—including crimes (or other illegal acts—Edelhertz's definition also reaches to acts that are prohibited by civil, administrative, or regulatory law, whether or not the perpetrators are ever called to answer for them) perpetrated outside of a business context, or by persons of relatively low social status.

Edelhertz identified four main types of white-collar offending: *personal crimes* ("[c]rimes by persons operating on an individual, *ad hoc* basis, for personal gain in a non business context"[8]), *abuses of trust* ("[c]rimes in the course of their occupations by those operating inside businesses, Government, or other establishments, or in a professional capacity, in violation of their duty of loyalty and fidelity to employer or client"[9]), *business crimes* ("[c]rimes incidental to and in furtherance of business operations, but not the central purpose of such business operations" [10]), and *con games* ("[w]hite-collar crime as a business, or as the central activity of the business"[11]).

The FBI, when it specifically addresses white collar crimes (nowadays, it usually references "financial crimes" instead[12]), uses a very similar definition:

---

7. HERBERT EDELHERTZ, THE NATURE, IMPACT AND PROSECUTION OF WHITE-COLLAR CRIME 3 (1970), *available at* https://www.ncjrs.gov/pdffiles1/Digitization/4415NCJRS.pdf. For various ways in which white collar crime has been manifested today, see G. Robert Blakey & Michael Gerardi, *Eliminating Overlap or Creating a Gap? Judicial Interpretation of the Private Securities Litgation Reform Act of 1995 and RICO*, 28 NOTRE DAME J.L. ETHICS & PUB. POL'Y 435 (2014) (discussing the intersection been the Racketeer Influenced and Corrupt Organizations Act with federal securities law and white collar crime); *see also* Cynthia A. Koller, Laura A. Patterson & Elizabeth B. Scalf, *When Moral Reasoning and Ethics Training Fail: Reducing White Collar Crime Through the Control of Opportunities for Deviance*, 28 NOTRE DAME J.L. ETHICS & PUB. POL'Y 549 (2014).

8. *Id.* at 19.

9. *Id.* at 19.

10. *Id.* at 20.

11. *Id.* at 20.

12. While the FBI has a white collar crime webpage, the crimes listed on it are various forms of fraud. However, these crimes are actually worked by the Financial Crimes Section. *See White Collar Crime,* FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/white_collar.

> The FBI focuses its financial crimes investigations on such criminal activities as corporate fraud, securities and commodities fraud, health care fraud, financial institution fraud, mortgage fraud, insurance fraud, mass marketing fraud, and money laundering. These are the identified priority crime problem areas of the Financial Crimes Section (FCS) of the FBI.

While they do not give an explicit definition of the term "financial crime," they do say, when talking about financial crimes, that "[t]hese crimes are characterized by deceit, concealment, or violation of trust and are not dependent upon the application or threat of physical force or violence. Such acts are committed by individuals and organizations to obtain personal or business advantage." *See* FED. BUREAU OF INVESTIGATION, FINANCIAL CRIMES REPORT TO THE PUBLIC FISCAL YEARS 2010–2011, *available at* http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011. This sounds very similar to the definition that the FBI used to give for white collar crime. *See* FED. BUREAU OF INVESTIGATION, WHITE COLLAR CRIME: A REPORT TO THE PUBLIC (1989).

> those illegal acts which are characterized by deceit, concealment, or violation of trust and which are not dependent upon the application or threat of physical force or violence. Individuals and organizations commit these acts to obtain money, property, or services; to avoid the payment or loss of money or services; or to secure personal or business advantage.[13]

This has been operationalized by the FBI's Criminal Justice Services Division to mean the Uniform Crime Report (UCR) offences of fraud, forgery/counterfeiting, embezzlement, and a rather longer list of National Incident-Based Reporting System (NIBRS) offenses.[14] Thus, while this definition and Edelhertz's are very similar, the FBI's definition functionally excludes non-criminal illegal activity, as well as such incidents as are not reported to police, and such incidents as do not fit into a relevant UCR or NIBRS category (for those jurisdictions that participate in NIBRS). On the other hand, the FBI's definition dovetails well with already-collected data, making it a practical tool for generating statistics on white collar crime activity.

As a practical matter, many people have rather informal interpretations of the term. White collar crime can refer to:

- Financial crimes
- Non-physical (or abstract) crimes
  - That is, crimes that "occur" on a form, balance book, or computer
- Crime by or targeting corporations
- Crimes typically committed by the rich
- Criminal businesses or organizations
  - Including, for some, organized crime and terroristic organizations
- Corporate or professional malfeasance
  - For some, this can include acts that are immoral, but that are not specifically prohibited by law (for example, an insurance company automatically targeting every policyholder who gets diagnosed with breast cancer for an aggressive fraud investigation to find any possible pretext to drop the account).[15]
- Anything that is against the law that the average beat cop would not typically handle
  - Essentially, everything but street crime

Finally, many people have a general sense that they know what counts as white collar crime and what does not, but have no specifically

---

13. FED. BUREAU OF INVESTIGATION, WHITE COLLAR CRIME: A REPORT TO THE PUBLIC, *supra* note 12.

14. Cynthia Barnett, *The Measurement of White-Collar Crime Using Uniform Crime Reporting (UCR) Data*, FED. BUREAU OF INVESTIGATION, at 2 (2000), *available at* http://www.fbi.gov/about-us/cjis/ucr/nibrs/nibrs_wcc.pdf.

15. *See* Murray Waas, *Corrected: WellPoint routinely targets breast cancer patients*, REUTERS (Apr. 23, 2010, 7:28PM), http://www.reuters.com/article/2010/04/23/us-wellpoint-breastcancer-idUSTRE63M5D42 0100423; *see also* Letter from Kathleen Sebelius, Sec'y of Health and Human Servs., to Angela Braly, WellPoint CEO (Apr. 22, 2010) (*available at* http://www.hhs.gov/news/press/2010pres/04/wellpoint04222010 .pdf).

articulated sense of what qualities separate members of the class from non-members.

B. *Attempts at Unifying Definitions*

Having so many definitions in use means that it is often difficult to compare data gathered by different white collar crime stakeholders, and that theoretical constructs in use by one group may be completely misaligned to the needs of another. One way that various groups have tried to reduce these inefficiencies is by crafting definitions that could enjoy buy-in from larger groups of stakeholders, providing them a common language (and compatible tools) for discussing white collar crime.

In 1996, the National White Collar Crime Center convened a group of noted academics specifically to address this definitional dilemma.[16] Attendees were selected from among the most noted scholars in the criminal justice field, who had devoted significant effort to the study of white collar crime. Several aspects of white collar crime were examined and discussed at length. Each attendee was asked to produce a paper on their position as to how the term should be defined, laying out their arguments in support of their preferred definition. From the presentation of these position papers, extensive discussions among the assembled academics were held. The result of the process was that white collar crime was examined from a variety of perspectives.

After considerable discussion and debate, those present at the workshop reached some consensus as to the elements that need to be present to satisfy the concept of white collar crime. Most agreed that the lack of direct violence against the victim was a critical element. They agreed the criminal activity should have been the result of an opportunity to commit the crime afforded by the offender's status in an organization or their position of respect within the community. They also agreed that deception to the extent necessary to commit the criminal offense (such as misrepresentation of the perpetrator's abilities, financial resources, accomplishments, some false promise or claim intended to deceive the victim, or possibly a deliberate effort to conceal information from the victim) should be considered an element of white collar crime. Some even took the position that we should do away with the term altogether and begin using something more along the lines of "economic crime," "elite crime," or simply "financial crime."[17]

---

16. A complete treatment of every position of every participant of the proceedings would be far beyond the scope of this Article. The citations that will follow, referring to those proceedings of 1996, were selected simply to help illustrate the magnitude of the problem of finding an acceptable definition. Inclusion or exclusion of mention of any of the participants is not intended in any manner to suggest that any single contribution was superior or inferior to another. The citations used were selected simply to represent the various perspectives from which the group examined the task of defining the concept of white collar crime.

17. *Proceedings of the Academic Workshop: Definitional Dilemma: Can and Should There Be a Universal Definition of White Collar Crime?,* NATIONAL WHITE COLLAR CRIME CENTER (1996); *see also* Gary R. Gordon, *The Impact of Technology-Based Crime on Definitions of White*

In the end, those in attendance ultimately agreed that white collar crime should be defined as "illegal or unethical acts that violate fiduciary responsibility of public trust, committed by an individual or organization, usually during the course of legitimate occupational activity, by persons of high or respectable social status for personal or organizational gain."[18]

C. *Working With Multiple Definitions*

It is important to point out that there is no such thing as the "right" white collar crime definition—only the definition that is right for the purposes of the entity employing it. It is, however, vital to understand what the term means to the person who is using it, in order to understand what they are actually saying. This can be especially important when dealing with abstracted statistics. The statement "white collar crime is increasing" is meaningless without understanding what white collar crime means to the author. The definition impacts what questions are asked, what kinds of answers are meaningful, and where researchers look for the answers to the questions. As has been noted by other researchers in the field, "[h]ow we define the term 'white-collar crime' influences how we perceive it as a subject matter and thus what and how we research."[19]

As the point of this Article is not to advocate for any particular interpretation of the term, we will be using the term "white collar crime" in the widest possible sense, so as not to exclude any of the various camps from the discussion. The definition that we will be adopting for the purposes of this Article, unless specifically indicated, is *wrongdoing that qualifies as white collar crime under any of the theoretical models described herein.*

II. White Collar Crime: Trends and Statistics

A. *Signs of a General Trend*

Despite the growing body of information concerning the frequency and costs of white collar crime, the true extent of the problem remains largely unknown. Estimates of the true costs of white collar crime vary greatly. Although the number is certainly high, it is extremely difficult to quantify. This can be attributed to a number of factors, including a lack of official statistical information and empirical studies devoted to the topic, disagreement as to which acts comprise white collar crime, and difficulty in capturing the data.

What is largely accepted as a given is that white collar crime is increasing, both in absolute numbers and compared to street crime.

Collar/Economic Crime: Breaking Out of the White Collar Paradigm, Utica College of Syracuse University 143, 144 (1996), *available at* http://www.jpsimsconsulting.com/site_media/cms_page_media/44/Definitional%20Dilemma.pdf.

18. Gordon, *supra* note 17, at 117–50.

19. David T. Johnson & Richard A. Leo, *The Yale White-Collar Crime Project: a Review and Critique*, The American Bar Foundation 63, 65 (1993).

Reputable data shows that traditional street crimes have been decreasing in frequency across the board for some time. The Bureau of Justice Statistics' victimization studies[20] show that, from 2002 to 2011, reported victimization by violent crime decreased by 22%, and reported victimization by property crimes decreased by 18%. Likewise, the Federal Bureau of Investigation's uniform crime reports [21] (which rely on police reports instead of victim data) show that rates of reports of violent crime decreased by 18.7% from 2003 to 2012, and rates of reports of property crime decreased by 20.4%. Meanwhile, there are signs that white collar crime should be on the increase:

1. The Skills Required to Commit White Collar Crimes are Becoming More Common

Many white collar crimes require significantly higher levels of education than street crimes, or specialized technical skills. All of these things are becoming more available in our society as we see a widespread increase in literacy rates,[22] computer use,[23] and educational attainment.[24]

20. Jennifer L. Truman & Michael Planty, *Criminal Victimization, 2011*, U.S. DEP'T OF JUSTICE, OFFICE OF JUSTICE PROGRAMS BULLETIN (Oct. 2012), http://www.bjs.gov/content/pub/pdf/cv11.pdf.

21. *Crime in the United States 2012*, FED. BUREAU OF INVESTIGATION, Tbl. 1A (2013), http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2012/crime-in-the-u.s.-2012/tables/1tabledatadecover viewpdf/table_1_crime_in_the_united_states_by_volume_and rate_per_100000_inhabitants_1993-2012.xls.

22. *World Illiteracy Rate 1970-2000 (prognosis for 2005-2015), age 15 years and over*, UNESCO INSTITUTE FOR STATISTICS, http://www.uis.unesco.org/en/stats/statistics/UIS_Literacy_Regional2002.xls (last visited Oct. 8, 2010) (showing that the illiteracy rate in America was 14.8% in 1970, and decreased to 6.9% in 2000).

23. *Computer and Internet Use in the United States 2009*, UNITED STATES CENSUS BUREAU, App'x Tbl. A: Households With a Computer and Internet Use: 1984 to 2009 (2013), *available at* http://www.census.gov /population/www/socdemo/computer/2009.html. Home computer ownership has grown from 8.2% of American households in 1984 to 61.8% of American households in 2003—the last year for which data was collected. Internet access at home grew from 18% of households in 1997 (the first year in which the question was asked) to 68.7% in 2009.

24. Kurt J. Bauman & Nikki L. Graf, *Educational Attainment: 2000*, U.S. CENSUS BUREAU 1, 4 fig.3 (Aug. 2003), http://www.census.gov/prod/2003pubs/c2kbr-24.pdf. The percentage of high school graduates increased from 24.5% of the American population to 80.4% of the population between 1940 and 2000. Similarly, the percentage of Americans with bachelor's degrees increased from 4.6% to 24.4% in the same period of time.

2. The American Populace is Aging

Physical crimes favor the young,[25] while fraud is generally associated with older perpetrators. [26]

3. Opportunity to Commit White Collar Crimes is Increasing

In traditional, "on the job" white collar crime, there was a time when only a very few individuals had access to the means to commit many white collar crimes. As recently as the 1960s, far less of America's work force had realistic access to corporate information. [27] By 2009, 86 million Americans were employed in management, professional, sales, and office professions, out of the total workforce of almost 140 million.[28] In other words, 61% of the total workforce now has potential access to trade secrets, corporate funds, and other targets of white collar crimes.

4. Things of Value are Increasingly Likely to be Intangible

Moving from means and opportunity to motivations, the nation is increasingly embodying its wealth in information or information products.[29] The value of a pirated CD is found in the information encoded on the disc, rather than in the cheap plastic medium itself. When the Business Software Alliance reports that $51.4 billion worth of software has been illegally copied ("pirated") in 2009,[30] they are reporting on the hypothetical value of lost sales of information—not on the loss of

25. James Alan Fox & Marianne W. Zawitz, *Homicide Trends in the United States*, BUREAU OF JUSTICE STATISTICS (2010), *available at* http://bjs.ojp.usdoj.gov/content/homicide/teens.cfm. Between 1975 and 2005, rates of homicide offending were consistently almost three times as high for Americans between eighteen and twenty-four as between twenty-five and thirty-four, about twice as high for Americans between twenty-five and thirty-four as between thirty-five and forty-nie, and almost negligible over forty-nine. In the aggregate, eighteen to thirty-four year olds were responsible for sixty-five percent of homicides during that period.

26. *Report to the Nations on Occupational Fraud and Abuse Global Fraud Study*, THE ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 1, 56–57 (2010), *available at* http://www.acfe.com/rttn/rttn-2010.pdf. Data from 2008 to 2010 shows that the majority of perpetrators of organizational fraud, worldwide, were between the ages of thirty-six and fifty. This data also shows that median damages rose with age.

27. *Comparative Civilian Labor Force Statistics, 10 Countries, 1960-2004*, U.S. DEP'T OF LABOR AND BUREAU OF LABOR STATISTICS 1, 30 tbl.7 (May 2005), *available at* http://www.bls.gov/fls/flslforc.pdf. From 1960 to 2004, agricultural employment fell from 8.4% to 1.6% of the total workforce. Industrial jobs fell from 33.4% to 20%. Manufacturing fell from 26.1% to 11.8%. Meanwhile, service employment rose from 58.1% to 78.4%.

28. *Household Data Annual Averages*, BUREAU OF LABOR STATISTICS, Tbl.9: Employed Persons by Occupation, Sex, and Age (2010), *available at* http://www.bls.gov/cps/cpsaat9.pdf.

29. Uday M. Apte, Uday S. Karmarkar & Hiranya Nath, *Information Services in the U.S. Economy: Value, Jobs, and Management Implications*, 50 CAL. MGMT. REVIEW 12, 17 (2008). Between 1967 and 1997, the share of the information economy in America's GNP is estimated to have grown from forty-six percent to sixty-three percent. It seems likely that this trend has continued in the thirteen years since this measurement was taken.

30. BUSINESS SOFTWARE ALLIANCE, SEVENTH ANNUAL BSA/IDC GLOBAL SOFTWARE 09 PIRACY STUDY 9 (2010), *available at* http://portal.bsa.org/globalpiracy2009/studies/globalpiracystudy2009.pdf.

the worth of the plastic discs (which they did not own and were likely legitimately purchased in the first place). The concept of wealth itself is increasingly represented in non-physical units. There was a time when, if thieves did not steal hard currency, they were invariably stealing something other than money. Now, money can be stolen through the manipulation of digital banking information stored in computer hard drives.

5. White Collar Techniques are Very Effective at Obtaining Intangible Things of Value

Things of value embodied in the form of information are particularly susceptible to attacks using information technology (computers). The rise of business computing means that a great deal of sensitive information that might once have been physically secured in locked cabinets or safes is now transmitted by email or stored on company servers. Although it is difficult to quantify the extent to which the underlying information is rendered more vulnerable by the use of digital storage and retrieval systems, it is a given that the system is tremendously more exposed. While both means of protecting the information could have theoretically equivalent levels of protection (including the digital equivalent of locks on the filing cabinet and building security, for example), the filing cabinet is only realistically exposed to criminal acts originating in the physical proximity of the office building, or from criminals who are willing to invest the resources to travel to the building. Contrariwise, a networked system is exposed to attack from anyone with an Internet connection, anywhere of the world, at any time.

Linking these computers together through the Internet has led to unprecedented potential for obtaining money through informational manipulation. Compared to "traditional" scam techniques, the Internet provides an incredibly cheap, relatively anonymous means of reaching potential victims. In the offline environment, a scam that only snares one target out of a thousand is unlikely to offer a high enough return on investment to be worth pursuing. On the other hand, the online version of that same scam can be enacted several thousand times at once with the use of a mailing list (or any other means of electronic mass distribution). If the criminal sends the opening gambit of the scam to twenty thousand potential victims, he or she may well get twenty useful replies in an afternoon. This is done with very little set-up cost, very little time investment, and relative anonymity compared to performing the scam in person. This also allows criminals to realistically pursue distributed victimization strategies, where the dollar loss is spread out across such a wide group of victims that no one case is worth investigating. A thousand geographically dispersed fifty dollar victimizations are presumably significantly less likely to be reported, much less investigated, than a single victimization of $50,000 would be.

This means that a single white collar criminal (or group of criminals) can easily be at the center of what seems like a world-wide crime wave. A single fraudster—like Robert Soloway, convicted in 2008

of fraud and criminal spamming—can completely flood the Internet with unsolicited and fraudulent emails. In Soloway's case, it was to the self-admitted tune of trillions of emails, which made him thousands of dollars a day[31] for a period spanning 1997 to 2007[32] (and for which he received a sentence of forty-seven months). Similarly, hacker Albert Gonzalez recently received a twenty-year sentence for leading a group of ten people who stole and then sold 40 million credit card numbers from customers of various companies that had unsecured wireless access points in the Miami area.[33]

Advanced information technologies and communication devices make white collar crimes easier to commit, while having little impact on street crime (as they are primarily used for interacting with nonphysical constructs, which is the general province of white collar crime). These technologies have become increasingly common across diverse social strata in recent years.[34] Unlike the portable communication technologies of the 1980s, they are no longer tools restricted to those who already possess comparatively high levels of wealth. This widespread adoption of these technologies in the United States is a positive sign in the vast majority of respects, but a logical consequence of increasing the online population is that there are more opportunities to either commit a white collar crime or become a victim of one.

While these factors give researchers confidence that white collar crime should be occurring in relatively large numbers (and should be growing at a time when other crimes are shrinking), proving it or putting a hard number on it is difficult. Relatively few studies attempt to assess the rate at which the public is victimized by white collar crime. The most recent comprehensive white collar crime victimization study (NW3C's 2010 National Public Survey on White Collar Crime[35]) found that 24.2% of American households in 2010 reported experiencing at least one form of white collar crime.[36]) It is worth noting that, in this case, the term "white collar crime" was operationalized to mean the following specific activities: credit card fraud, price fraud, repair fraud,

31. Jim Popkin, *'Pure Greed' Led Spammer to Bombard Inboxes*, NBC NEWS (Sep. 22, 2008), http://www.msnbc.msn.com/id/26797741/.

32. J. Sullivan, *Government's Sentencing Memorandum no. cr07-187mjp, U.S. v. Soloway* (July 2008), *available at* http://www.spamsuite.com/webfm_send/338.

33. Sheri Qualters, *Computer Hacker Albert Gonzales Sentenced to 20 Years*, NAT'L L. J. (Mar. 2010), http://www.law.com/jsp/article.jsp?id=1202446860357&rss=newswire.

34. Kathryn Zickuhr & Aaron Smith, *Digital Differences*, PEW INTERNET, at 8 (Apr. 13, 2012), http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf (the "Digital Divide" report series illustrates a continuous, steady decrease in the gap between broadband adoption levels for different races and different income levels). For that matter, minority members actually outpace Caucasians in both cell-phone ownership and use of cell phones to go online. Maeve Duggan & Aaron Smith, *Cell Internet Use 2013*, PEW INTERNET (Sep. 16, 2013), http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_CellInternetUse2013.pdf.

35. RODNEY HUFF, CHRISTIAN DESILETS, & JOHN KANE, NATIONAL WHITE COLLAR CRIME CENTER, THE NATIONAL PUBLIC SURVEY ON WHITE COLLAR CRIME 22 (2010), *available at* http://crimesurvey.nw3c.org /docs/nw3c2010survey.pdf.

36. Compare that statistic to the fact that 12.5% of all households being victimized by property crime in that same year. Truman & Planty, *supra* note 20.

Internet fraud, business fraud, securities fraud, and mortgage fraud (so this data says nothing about embezzlement rates or regulatory violations, for example).

That is not to say that data has not been gathered on other aspects of white collar crime. For example, the National Crime Victimization Survey has found that 7% of American households were victimized by identity theft in 2010.[37] Similarly, the Federal Trade Commission has administered surveys devoted to assessing the prevalence of various types of consumer fraud (10.8% of American adults were victimized in 2011).[38]

B. *Limitations of the Data*

While data on various forms of white collar crime is available, it is important to understand what this data can and cannot say. The data that we will be discussing in the rest of the Article has problems when dealing with any of the following factors:

- Undetected behavior
  - Respondents can only report on crimes that they are aware of
  - Example: Fraudulent schemes that are presumed to be legitimate at the time of the study
- Criminal behavior erroneously perceived to be an exclusively civil matter
  - The public sometimes has an inaccurate idea of what sort of behavior may be considered criminal
  - Example: Contractors billing for work that was not performed, when characterized as a contract dispute instead of fraud.
- Known and detected crimes where the respondent is unaware that they are a victim
  - Unlike most street crimes, white collar crimes can victimize large, poorly-defined categories of people
  - Example: An instance of price-fixing within an industry segment, where the perpetrators are convicted of the crime but little effort is put into educating consumers about whether the products that they purchased were among those whose prices were illegally manipulated.
- White collar crimes of types that were not asked about
  - Having different definitions from one researcher to another means that it is not uncommon to find that statistics that purport to describe white collar crime only describe a relatively narrow portion of it.
  - Example: Many white collar crime statistics assume that the rate of white collar crime is equal to the rate of frauds

37. LYNN LANGTON, U.S. DEP'T OF JUSTICE: OFFICE OF JUSTICE PROGRAMS, IDENTITY THEFT REPORTED BY HOUSEHOLDS, 2005–2010, at 1 (2011), *available at* http://www.bjs.gov/content/pub/pdf/itrh0510 .pdf.

38. KEITH B. ANDERSON, FED. TRADE COMM'N, CONSUMER FRAUD IN THE UNITED STATES, 2011: THE THIRD FTC SURVEY 17 (2013).

reported to police (ignoring counterfeiting, embezzling, securities violations, etc.).

- Detected and correctly identified criminal acts that were asked about and of which the respondent realizes that they are a victim, but about which the respondent does not choose to speak
  - All surveys that rely on the answers of respondents are dependent on the respondents answering honestly. While surveys can be designed to reduce the motivation for giving false answers (for example, by being anonymous and by being administered by a surveying firm with no stake in the results favoring any particular view), any respondents who give false information—either hiding true incidents or inventing false ones—necessarily make it harder to see the actual underlying patterns in the data.
  - Example: A victim of a scam, who now feels foolish for being taken in, is too embarrassed to tell researchers about the incident.
- Detected and correctly identified criminal acts, where the victim prefers to pursue financial compensation rather than penal sanctions.
  - For non-survey data (such as that obtained from police reports), the data can be skewed by unintentional incentives or penalties for using various reporting systems. Prior studies have shown that, while white collar crime victimization seems to be on the rise, such victimization is reported at a much lower rate than traditional crimes. Moreover, even fewer of the white collar crimes reported actually land in the hands of a crime control agency. [39] NW3C's studies have found that only 11.9% of white collar crimes are ever reported to an agency with any sort of law enforcement power,[40] compared with about 50% of violent crimes and 37% of property crimes being reported to the police.[41]
  - Example: A consumer who finds that their credit card has been used to make unauthorized purchases online—reporting it to their bank carries with it a good chance that they will be reimbursed and the fraud will stop. Reporting it to the police carries with it the relatively larger transactional costs of dealing with the government (whose investigation may also prove to be intrusive, embarrassing, or burdensome to the victim) and often has no direct benefit to the consumer.

C. *Specific Crimes and What We Know About Them*

Because there are many different definitions of white collar crime, there is no list of activities that categorically "are" white collar crimes.

39. Richard M. Titus, Fred Heinzelmann & John M. Boyle, *Victimization of persons by fraud*, 41 CRIME & DELINQUENCY, 1, 54 (1995).

40. HUFF, DESILETS & KANE, *supra* note 35, at 25.

41. Truman & Planty, *supra* note 20, at 8.

However, there are many types of activities that could be included, at least partially, under a relatively large number of definitions. A brief overview of some of these general categories follows. These categories are neither exhaustive nor mutually exclusive.

Of course, none of the crimes that are listed here are relevant to a definition that hinges upon the qualities of the offender. This is not because of a lack of professional or academic interest in these sorts of offenders, but because empirical data on the subject (from that angle) has not been gathered in any sort of large-scale, systematic way. As Sherlock Holmes once said, one "can't make bricks without clay." [42]

1. Consumer Crimes

The category of consumer crimes includes, but is not limited to, false advertising, commercial misrepresentations, price manipulation, and related criminal and/or unethical behaviors. Few statistics address the entire group, as the white collar crime stakeholders who would be the motive force behind such data collection tend to focus on narrower questions. As in many other types of white collar crime, much of the data is also fragmented between the civil, administrative, and criminal routes. However, existing data suggests that enforcement of these matters is at least on the rise. For example, the number of federal actions each year under the False Claims Act more than doubled from 1987 to 2012,[43] and the number of complaints to FTC's Consumer Sentinel Network increased more than six-fold from 2001 to 2012.[44] Whether this is because of an increase in the underlying activities, an increase in the likelihood of each victim reporting their victimization, or an increase in law enforcement interest or ability to combat the activities is unknown.

2. Intellectual Property Crimes

Intellectual property, as a concept, covers patent law, copyright law, trademark law, and trade secret law. With that said, intellectual property crimes tend to be of one of two types:

Criminal versions of trademark dilution claims: Claims that an item creates the likelihood of confusion as to the source of the product

Criminal versions of copyright infringement laws: Unsanctioned copying of creative material created by another.

---

42. ARTHUR CONAN DOYLE, THE ADVENTURES OF SHERLOCK HOLMES: THE ADVENTURE OF THE COPPER BEECHES 322 (1892) ("As to Holmes, I observed that he sat frequently for half an hour on end, with knitted brows and an abstracted air, but he swept the matter away with a wave of his hand when I mentioned it. 'Data! data! data!' he cried impatiently. 'I can't make bricks without clay.' And yet he would always wind up by muttering that no sister of his should ever have accepted such a situation.").

43. *Fraud Statistics—Overview: October 1, 1987—September 30, 2012, Civil Division*, U.S. DEP'T OF JUSTICE: CIVIL DIV. (Oct. 24, 2012), http://www.justice.gov/civil/docs_forms/C-FRAUDS_FCA_ Statistics.pdf.

44. FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 5 (2013), *available at* http:// ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

a. Trademark-Related Claims

Counterfeit Merchandise

It can be difficult to decide which metrics are relevant when looking at data on counterfeit merchandise. For example, the U.S. government seized $178 million in counterfeit and pirated merchandise in 2011, [45] a 5% decrease from the year before and a 35% decrease from 2008.[46] One could use this figure to show that counterfeiting is decreasing. On the other hand, that figure represents 24,792 seizures, which is the most on record (24% higher than the year before and 4.5 times higher than the number of seizures in 2002). [47] Finally, the number of these seizures that were deemed "consumer safety and critical technology" seizures increased 44% over the year before, and the value of these seizures increased 41% over the year before (to $60 million).

These figures, however, only refer to those incidents of counterfeiting that the federal government detected and stopped (typically at a port or border). Many counterfeit goods either make it through these checkpoints or are manufactured domestically, and are then sold throughout the nation. While hard figures on such operations do not exist, the Organization of Economic Cooperation and Development (OECD) estimated total U.S. losses to counterfeiting and piracy at over $250 billion.[48]

Counterfeit Pharmaceuticals

While almost any counterfeit good may potentially pose a health and safety risk, pharmaceutical counterfeiting is a topic of special concern. Recent studies suggest that only 38% of online pharmacies are selling authentic versions of the medications that they offer. [49]

According to the most recent estimates, 6.8 million Americans are actively using prescription drugs for non-medical reasons, [50] accounting for more than a quarter of all illicit drug use in America. When it comes to illicit drugs, pharmaceuticals are second only to marijuana in

45. U.S. Customs & Border Protection & U.S. Immigration & Customs Enforcement, Intellectual Property Rights: Fiscal Year 2011 Seizure Statistics 6 (2012), *available at* http://www.iprcenter.gov/reports/ipr-center-reports/2011-seizure-statistics/view?vm=r.

46. U.S. Customs & Border Protection & U.S. Immigration and Customs Enforcement, Intellectual Property Rights: Seizure Statistics-Fiscal Year 2009, *available at* http://cbp.gov/xp /cgov/trade/priority_trade/ipr/seizure/.

47. U.S. Customs & Border Protection & U.S. Immigration & Customs Enforcement, *supra* note 45, at 6.

48. Organisation for Economic Co-operation and Development, Magnitude of Counterfeiting and Piracy of Tangible Products: An Update 1 (2009), *available at* http://www.oecd.org/dataoecd/57/27/44088872.pdf.

49. European Alliance for Access to Safe Medicines, The Counterfeiting Superhighway, 27 (2008), *available at* http://v35.pixelcms.com/ams/assets/3122966785 31/455_EAASM_counterfeiting%20report_020608.pdf.

50. *Results from the 2012 National Survey on Drug Use and Health: Summary of National Findings*, Substance Abuse and Mental Health Services Administration, NSDUH Series H-46, HHS Publication No. (SMA) 13-4795, at 14 (Sep. 2013), *available at* http://www.samhsa.gov/data/NSDUH/2012SummNatFindDetTables/NationalFindings/NSDUHresults2012.htm#ch2

popularity.[51] What is more, the relative figure seems unlikely to fluctuate much in the future—the proportion of Americans over 12 who reported using prescription drugs for nonmedical reasons in the past month has held fairly stable (vacillating between 2.4% and 2.9%) for as long as the current incarnation of the National Survey on Drug Use and Health has existed (since 2002).[52]

At the same time, the health impact seems to be growing more severe. Emergency room admissions for misuse of prescription drugs (especially opiate painkillers[53]) more than doubled from 2004 to 2009.[54] The rate of drug-related accidental poisoning deaths has increased by 130% from 1999 to 2007. [55] The rate of drug-related accidental poisoning deaths has increased by 130% from 1999 to 2007.[56] Nearly ninety-four percent of the unintentional poisoning cases that resulted in death during that period were drug-related.[57] Death by accidental poisoning related to drugs has become the second most common type of unintentional injury resulting in death. [58] It is the thirteenth most common cause of death (from any source) in the

51. *Id.* (statistics show for past-month users in 2002: pharmaceuticals at 6.8 million, marijuana at 18.9 million, and illicit drugs of any type at 23.9 million).

52. *Id.* at 15. In 2012, there were 6.8 million (2.6%) persons aged 12 or older who used prescription type psychotherapeutic drugs nonmedically in the past month. These estimates were higher than in 2011 (2.4%) but similar to estimates in 2010 (2.7%), 2009 (2.8%), 2008 (2.5%), 2007 (2.8%), 2006 (2.8%), 2005 (2.6%), 2004 (2.5%), 2003 (2.7%), 2002 (2.6%).

53. Admissions for nonmedical use of prescription opiates in particular increased 141% from 2004 to 2009. There were 172,726 such admissions in 2004, and 416,458 in 2009. *Drug Abuse Warning Network, 2009: National Estimates of Drug-Related Emergency Department Visits*, SUBSTANCE ABUSE AND MENTAL HEALTH SERVICES ADMINISTRATION CENTER FOR BEHAVIORAL HEALTH STATISTICS AND QUALITY, HHS Publication No. (SMA) 11-4659, DAWN Series D-35, at 55 (Aug. 2011), *available at* https://dawninfo.samhsa.gov/data/ed/Nation/Nation_2009_NMUP.xls.

54. *Id.* There were 536,247 visits in 2004; 855,838 visits in 2007 and 1,079,683 visits in 2009.

55. *Compressed Mortality File 1999-2007, Series 20 No. 2M*, CTR. FOR DISEASE CONTROL (2010), *available at* http://wonder.cdc.gov/cmf-icd10.html. The death rate for ICD-10 codes X40-X44 was 4.0 per 100,000 in 1999, and has steadily risen to 9.2 per 100,000 in 2007.

56. *Id.* The death rate for ICD-10 codes X40-X44 was 4.0 per 100,000 in 1999, and has steadily risen to 9.2 per 100,000 in 2007.

57. *Id.* 166,923 of the 177,973 deaths that listed accidental poisoning as the cause of death (ICD-10 codes X40-X49) fell within codes X40-X44 (covering various forms of drugs).

58. 10 Leading Causes of Nonfatal Injury, United States, OFFICE OF STATISTICS AND PROGRAMMING, NAT'L. CTR. FOR INJURY PREVENTION & CONTROL, CTR. FOR DISEASE CONTROL & PREVENTION, http://www.cdc.gov/ncipc/wisqars/nonfatal/quickpicks/quickpicks_2007/allinj.htm (last visited Apr. 27, 2014). There were 29,846 fatalities for unintentional poisoning in 2007 (compared to top ranked motor vehicle traffic, which claimed 42,031 lives that year). This represents 24.1% of all accidental deaths in that year. Of these deaths, 27,658 of them (92.7%) are attributable to ICD-10 codes X40-X44 (which correspond to prescription drug abuse, though they would also cover non-prescription drugs- heroin and opiate pain relievers fall under the same category. Thus, accidental poisoning related to prescription drug use actually accounts for 22.4% of all accidental deaths. This is still more than #3 ranked falling, with 18.3% of deaths.)

nation,[59] responsible for 75% more deaths than murder.[60] It is also the tenth most common cause of nonfatal injuries overall. [61]

The data does not exist at this time to conclusively link the rise in physical harm caused by prescription drugs to the prevalence of counterfeit medication (whether sold online or otherwise). However, the fact that injuries are increasing at a time when use is holding steady strongly suggests the influence of some outside factor, and the emergence and prevalence of the counterfeit online pharmaceutical industry seems, at the very least, unlikely to be completely unrelated.

b. Copyright-Related Claims

Software, Movie, and Music Piracy

The Business Software Alliance estimates that losses due to pirated software in 2011 reached $9.8 billion for the U.S (with a piracy rate of 19%),[62] with global losses reaching $63.4 billion and a global piracy rate of 42%.[63] These figures indicate a steady upward climb from previous years (global piracy, for example, accounted for $30 billion in 2003). However, it is worth noting that the high dollar figures cited do not necessarily translate into lost sales. It is not a given that, but for lax enforcement, the industry would have made an extra $63.4 billion in 2011—many of the infringers would likely not have purchased a copy of the software at retail price. Additionally, it is difficult to characterize these figures as representing damages, as it is hard to articulate a type of damage unsanctioned copies impose other than lost sales (since creating a copy of a program does nothing to diminish the original). There are, however, some known cases of malware being hidden in pirated copies of software. Whether these isolated incidents constitute a trend, or how much impact they have had, is a topic for future research.

The movie and music industries have similar hurdles to surmount when trying to describe the size and impact of piracy in their sectors. However, the Motion Picture Association of America cites figures of $22 billion damage to U.S. industries in 2005 due to film piracy (or, possi-

59. *WISQARS Details for Leading Causes of Death*, OFFICE OF STATISTICS AND PROGRAMMING, NAT'L. CTR. FOR INJURY PREVENTION AND CONTROL, CTR. FOR DISEASE CONTROL AND PREVENTION (Apr. 28, 2011), *available at* http://webappa.cdc.gov/sasweb/ncipc/leadcaus10.html. Breaking out the various types of unintentional injuries instead of lumping them together into one category, accidental death by motor vehicle traffic becomes the #9 most common cause of death (beating out septicemia with 34,828 deaths) and death by accidental poisoning relating to prescription drugs (ICD-10 codes X40-X44) becomes the new #13, beating out hypertension with 23,965 deaths.

60. According to the FBI's Uniform Crime Report for 2007, there were 15,707 murders in that year. *See Crime in the United States, 2007*, FED. BUREAU OF INVESTIGATION (Sep. 2008), http://www2.fbi.gov/ucr/cius2007/data/table_12.html.

61. Accidental poisoning accounted for 679,890 nonfatal injuries in 2007. *See WISQARS Details for Leading Causes of Death*, *supra* note 59.

62. *Shadow Market: 2011 Global Software Piracy Study*, BUS. SOFTWARE ALLIANCE (May 2012), http://globalstudy.bsa.org/2011/downloads/opinionsurvey/survey_us.pdf.

63. *Id.*

bly, $6.1 billion),[64] and the Recording Industry Association of America cites figures of $12.5 billion lost annually.[65]

3. Business and Financial Crimes

Financial crimes, in this sense, are those crimes that "occur on the balance-book," a concept that can cover a wide array of behaviors. Judging the size of these sorts of crimes is difficult. On the one hand, the victimization rate is arguably something close to 100%, if you consider the recent economic downturn to be directly linked to criminal or unethical economic activity. On the other hand, it is incredibly hard to untangle this sort of activity from the business cultures that birth it, and these selfsame cultures tend to generate their own behavioral norms that are not necessarily congruent with the norms of the society in which they exist. Does the dishonesty inherent in the used car salesman (or lawyer, or politician) trope acknowledge a pattern of systemic corruption within the profession, or is it a signal of societal acceptance of the concept that certain roles within the society require different degrees of latitude? Or, to put it differently, does anyone really expect a used car salesman to be able to survive (much less thrive) in their profession by fully and honestly disclosing all relevant information? While the clandestine nature of frauds, thefts, and other illicit behaviors are always a complicating factor in detecting and quantifying such crimes, these things are at least typically understood to be wrong and can therefore be reported to authorities when they are discovered (though, as discussed earlier, even that is done at a very low rate). Hidden behavior that is not understood to be wrong, or that is tacitly encouraged, is presumably even less likely to be reported or punished.

One particularly illustrative example of this is in the person of Ivar Kreuger, "The Match King."[66] In post-WWI Europe, he undertook a number of practices that would currently be considered criminal but that, at the time, were at worst questionable. He pioneered the practice of vastly overstating his assets, becoming somewhat famous for orchestrating a takeover of a significantly larger rival by making them think

64. DANIEL CASTRO, INFORMATION TECHNOLOGY & INNOVATION FOUND., BETTER ENFORCEMENT OF ONLINE COPYRIGHT WOULD HELP, NOT HARM, CONSUMERS (2010), *available at* http://www.itif.org/files/2010-copyright-coica.pdf. This report cites a report that the MPAA does not directly link to as support for a $20 billion figure for total damage to the U.S. economy, and then, without explanation, adds $2 billion to it to account for U.S. retailers. *See also* STEPHEN E. SIWEK, INST. FOR POLICY INNOVATION, THE TRUE COST OF COPYRIGHT INDUSTRY PIRACY TO THE U.S. ECONOMY (2006), *available at* http://www.ipi.org/docLib/20120117 _CostOfPiracy.pdf. This report comes to the $20 billion figure by taking a more modest $6.1 billion figure found by earlier studies and factoring in a number of multipliers to estimate the downstream effects that lost film revenues might have on the economy.

65. *About Piracy*, RECORDING INDUS. ASSOC. OF AM., http://www.riaa.com/physicalpiracy.php?content_selector=piracy_details_street (citing the same company and author used by the MPAA). *See* SIWEK, *supra* note 64. This study doesn't have access to the sorts of base numbers that informed the MPAA study, but still creates an overall downstream damage estimate in a similar fashion.

66. *Christmas Specials: Fraud and financial innovation: The match king*, ECONOMIST, Dec. 22, 2007, at 77.

that his company was much larger than it was. He hid significant debts through the use of entities that were not listed on his companies' balance sheets—a tactic also favored by Enron's Lehman Brothers. He delivered unsustainable returns on investments to make his business seem artificially prosperous (he paid dividends out of capital instead of earnings). He gave and promised money (making large loans to cash-strapped European nations after WWI) that he did not have. On the other hand, he is also credited with a host of financial innovations (such as inventing the B-share). The "Kreuger Crash" of 1932 (when his true financial state became known, rendering his stocks and debentures essentially worthless) heavily influenced the U.S. Securities Acts of 1933 and 1934 (the first federal attempts to regulate securities, created in response to this and the stock market crash of 1929). These set new standards for disclosure of material information to stockholders in large part because of how artfully he hid needed information from investors. He was, and still is, hailed as a financial innovator and pioneer, and many of his techniques and inventions are still in use today. But apart from the forging of Italian bonds, it is unclear at what point, if any, his lying and maneuvering crossed over from savvy corporate helmsmanship to outright fraud.

From that perspective, the projected scope of business and financial crimes is almost inconceivably vast. The total costs of the Great Recession (which was caused, in part, by illegal or unethical lending and securities practices[67]) are estimated to be between 6-14 trillion dollars.[68] This is potentially higher than the U.S. Gross Domestic Product for 2007 (13.06 trillion dollars),[69] and it only reflects the damage done by corruption in one sector, albeit a sector that has a large impact on the American economy.

Another recent high profile case is the collapse of the Enron Corporation. In this example, the company was engaged in a complex scheme that involved conspiring with their highly respected accounting firm, Arthur Andersen, to shift massive debts to off-the-books partnerships controlled by Enron insiders, thereby allowing Enron to grossly misrepresent its income flow and profits.[70] A related case involved the conviction of the Arthur Andersen accounting firm that represented the Enron Corporation. One of the "Big Five" accounting firms, Arthur Andersen employed more than 85,000 employees worldwide. The result of the convictions resulted in the total disintegration of a company that had been in business for eighty-nine years.[71] Thousands of investors and pensioners lost billions of dollars (investors were attrib-

67. THE FINANCIAL CRISIS INQUIRY COMM'N, THE FINANCIAL CRISIS INQUIRY REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON THE CAUSES OF THE FINANCIAL AND ECONOMIC CRISIS IN THE UNITED STATES (2011).

68. David Luttrell, Tyler Atkinson, & Harvey Rosenblum, *Assessing the Costs and Consequences of the 2007-2009 Financial Crisis and its Aftermath*, ECONOMIC LETTER VOL. 8, NO. 7 (Sept. 2013), http://dallasfed.org/research/eclett/2013/el1307.cfm.

69. *United States Economy 2007*, 2007 CIA WORLD FACTBOOK, http://www.allcountries.org/wfb2007 /united_states/united_states_economy.html?vm=r.

70. E. JENSEN & J. GERBER, ENCYCLOPEDIA OF WHITE COLLAR CRIME (2007).

71. *Id.*

uted as collectively losing $74 billion,[72] $67 billion was owed to creditors,[73] and $2 billion was lost from employee pensions[74]) as a result of these illegal acts.

Operating in a similar timeframe was Bernard Madoff, who committed what is generally considered the largest scale Ponzi scheme in history. He was an investment broker and dealer who attracted new clients by showing consistent, strong returns of around 10% per annum—when, in fact, he had stopped actually executing trades in the early 1990's. In December 2008, Madoff confessed to the FBI that he had been operating his Ponzi scheme for over a decade.[75] In total, his scams caused an estimated $18 billion in damages [76]

Within these patterns of systemic tolerance for otherwise criminal behavior, some actions stand out as criminal even by their own standards. The FBI's Financial Crimes Section experienced a 37% increase in corporate crime cases from fiscal year 2007 to fiscal year 2011, a 51% in securities and commodities fraud cases, a 124% increase in mortgage fraud cases (though that was down 14% from a record high in fiscal year 2010) and a 45% decrease in money laundering cases.[77]

It should be cautioned, however, that an increase in rates of enforcement does not necessarily reflect an increase in the underlying activity—especially in the climate of 2007, in which the public was first starting to look for people on whom to place the responsibility for the mortgage crisis. Likewise, it is unknown whether the decrease in money laundering cases reflected a decrease in money laundering activity, an increase in the ability of state and local police to handle the cases, or simply a decrease in available manpower as agents in the section were assigned to the various case types whose prevalence was increasing.

a. Embezzlement

The topic of financial crimes being so vast, it helps to break it down into smaller, more focused crime concepts. For the sake of illustration we can examine a bit of research performed here at NW3C in early 2013. The original research goal was to examine embezzlement to

72. Kris Axtman, *How Enron awards do, or don't, trickle down*, CHRISTIAN SCIENCE MONITOR (June 20, 2005), http://www.csmonitor.com/2005/0620/p02s01-usju.html.

73. *Enron's Plan Would Repay a Fraction of Dollar's Owed*, N.Y. TIMES, July 12, 2003, at A1.

74. James Doran, *Enron Staff win $85m*, TIMES (U.K) (May 14, 2004), http://www.webcitation.org/5tZ5myXGx.

75. Diana B. Henriques, THE WIZARD OF LIES: BERNARD MADOFF AND THE DEATH OF TRUST (2011).

76. *The Madoff Scam: Meet the Liquidator*, CBSNEWS (June 10, 2010), http://www.cbsnews.com/stories/2009/09/24/60minutes/main5339719.shtml?tag=currentVideoInfo;segmentUtilities.

77. FED. BUREAU OF INVESTIGATION, FINANCIAL CRIMES REPORT TO THE PUBLIC FISCAL YEARS 2010-2011, (2011), *available at* http://www.fbi.gov/stats-services/publications/financial-crimes-report-2010-2011. For a discussion on money laundering prosecutions, see Leslie A. Dickinson, Note, *Revisiting the "Merger Problem" in Money Laundering Prosecutions Post-*Santos *and the Fraud Enforcement and Recovery Act of 2009*, 28 NOTRE DAME J.L. ETHICS & PUB. POL'Y 579, 590 (2014).

determine if it were possible to profile this crime in the same manner as one might profile a serial murderer. Embezzlement being a relatively broad category, we decided to limit the information gathering to cases involving embezzlement in public education. We compiled a sample of 300 cases of embezzlement in the public schools during calendar year 2012, reported either in the media or posted on the many State Attorney General web sites available on the Internet.

The results showed, among other findings, that of those responsible, 30% were clerical staff who had been entrusted with access to finances, 17.6% were elected officials (either school board members or officers of a parent teachers association), 41% were in management positions (not elected), 4% were students fraudulently applying for student loans, 2% were volunteers serving in a clerical capacity with access to funds, and 2% were vendors.[78] The breakdown of the perpetrators by gender was 60% female and 40% male. Unfortunately, the sources did not contain sufficient information to examine levels of education, income, criminal history, etc. The most alarming statistic derived from this sample was that the total dollar amount amounted to $180,198,702.36.

One is left to assume that given the positions of trust that allowed the majority (only 8% of the known perpetrators were students, volunteers or vendors) of these people to carry out their crime, they were not embezzling to provide for basic human needs of food clothing and shelter. As the typical offender embezzled within the course of a white-collar occupation, it is reasonable to categorize the majority of the perpetrators as persons of 'respectability,' if not some social status.

Taken individually, some of the actors in the sample cases embezzled only a few hundred dollars out of a petty cash fund while one of the high end examples of embezzlement stole $26.7 million (discovered by a state audit of a school district in Massachusetts). In the case of the embezzlements of a few hundred dollars, the perpetrators occupied positions of trust, relatively respectable social status, carried out the crime in secrecy, and [until discovered] never actually confronted the victims (who did not realize that they had suffered a loss until the crime was discovered). In the case of the multi-million dollar embezzlement, the situation was exactly the same except for the dollar amount stolen and the status of the person(s) involved in the commission of the crime. In that case, the position of respectability was significantly more pronounced (members of the Board of Education).

4. Terrorism

Although not strictly speaking a variety of white collar crime so much as an instance of it, it is worth noting that white collar crime is not exclusively the domain of bankers. It is also one of the tools at the disposal of terrorists. Prior to the September 11th terrorist attacks, the

78. *Id.* The total does not equal 100%, due to the fact that there were some cases cited where either a perpetrator was not named in the source, or the investigation failed to determine a perpetrator.

tracking and interdiction of "terrorist financing was not a priority for either domestic or foreign intelligence."[79] Since that day, however, it has become clear that understanding terrorist financing is a key—if not *the* key—component to combating terrorism. Although the terrorist attacks alone may not seem expensive on the surface, the volume of monetary support needed to sustain terrorist training camps, control centers, and infrastructure is high.[80] Not only does the termination of terrorist financing rob terrorists of the ability to fund their activities, but "tracking the movement of funds among individuals in terrorist groups and their supporters provides verifiable indications of associations, relationships, and networks."[81] This information is vital to successful investigations of such activity.

The varied nature of terrorist financing makes the tracking and interdicting of this activity difficult. It is well known that modern terrorists employ extremely varied, often quite common crimes in an effort to not only generate but to move and obscure the flow of funds. For example, it has been observed that some terrorist cells are funded by organized crime efforts such as cigarette smuggling, illicit drug running, and the fencing of stolen baby formula, while other examples of terrorist financing endeavors include heavy reliance on white collar crimes, such as fraud, identity theft, and intellectual property theft.[82] Terrorists have used fraudulent charitable organizations claiming to support a particular cause, such as disaster relief or food services, in order to generate money for their cause.[83]

In a sample of terrorism defendants indicted in federal court since September 11, 2001,[84] 54% were charged with a form of identification document fraud,[85] 16% were charged with a form of financial fraud,[86] 10% with credit card fraud, and 4% with mail or wire fraud. [87]

---

79. JOHN ROTH, DOUGLAS GREENBURG, & SERENA WILLE, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, MONOGRAPH ON TERRORIST FINANCING, *available at* http://govinfo.library.unt .edu/911/staff_statements/911_TerrFin_Monograph.pdf.

80. PATRICK D. BUCKLEY & MICHAEL J. MEESE, THE FINANCIAL FRONT IN THE GLOBAL WAR ON TERRORISM.

81. *Id.* at 3.

82. DEAN T. OLSON, FED. BUREAU OF INVESTIGATION, FINANCING TERROR (2007), *available at* http://www. au.af.mil/au/awc/awcgate/fbi/financing_terror.pdf.

83. United States v. Arnaout, 431 F.3d 994 (7th Cir. 2005). *See also* Holy Land Found. for Relief and Dev. v. Ashcroft, 333 F.3d 156 (D.C. Cir. 2003).

84. JOHN KANE & APRIL WALL, NAT'L WHITE COLLAR CRIME CENTER, IDENTIFYING THE LINKS BETWEEN WHITE-COLLAR CRIME AND TERRORISM (2004) (unpublished report on file with the U.S. Dept. of Justice).

85. Including fraud in connection with identification documents and information (18 U.S.C. § 1028 (2012)), forgery or false use of a passport (18 U.S.C. § 1543 (2012)), misuse of a passport (18 U.S.C. § 1544 (2012)), and fraud and misuse of visas, permits, and other documents (18 U.S.C. § 1546 (2012)).

86. Including bank fraud (18 U.S.C. § 1344 (2012)), money laundering (18 U.S.C. § 1956 (2012)), structuring financial transactions (31 U.S.C. § 5324 (2012)), making a false statement on a credit application (18 U.S.C. § 1014 (2011)), counterfeiting or forging securities of the states and private entities (18 U.S.C. § 513 (2012)), operating an unlicensed money transmitting business (18 U.S.C. § 1960 (2012)), and racketeering (18 U.S.C. § 1962 (2012)).

There is also the possibility that white collar crimes might become, themselves, vectors for terrorism, espionage, or warfare. Ninety percent of all data breaches in 2012 (that came to the attention of the Verizon Security Team) were attributable to state-affiliated actors tied to China.[88]

5. Computer Crimes

The use of technology to facilitate or initiate consumer fraud is now so commonplace that 50% of all consumer frauds reported to the FTC in 2012 were web or e-mail based.[89]

The average annual cost per victim (including direct, indirect, and opportunity costs) of cybercrime targeting organizational victims in the United States was $11.6 million in 2012 (up 26% from the year before).[90] While any estimate for overall losses stemming from clandestine activity is necessarily hindered by a lack of data, best estimates currently put annual net U.S. losses attributable to cybercrime in the neighborhood of $100 billion.[91]

Additionally, the Verizon Incident Response Team handled more than 47,000 security incidents, representing more than 44 million compromised files, in 2012. Fifty-five percent of those incidents ultimately resolved back to organized criminal organizations, and 21% resolved back to state-affiliated espionage. Thirty-seven percent of these breaches affected financial organizations, and 24% affected retail establishments. Seventy-five percent were driven by financial motives.[92]

JP Morgan's 2012 Cyber Source Online Fraud Report estimates that $3.4 billion was lost to Internet fraud. According to their 13th annual survey, "merchants reported losing an average of 1.0% of total online revenue to fraud." It is stated that international orders are more risky than domestic orders. Merchants reported the international fraud

87. Including mail fraud (18 U.S.C. § 1341 (2012)) and fraud by wire, radio, or television (18 U.S.C. § 1343 (2012)).

88. VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT 5 (2013).

89. FED. TRADE COMM'N, CONSUMER SENTINEL NETWORK DATA BOOK 9 (2013), *available at* http://ftc.gov/sentinel/ reports/sentinel-annual-reports/sentinel-cy2012.pdf.

90. It's worth noting that these results are not necessarily generalizable to all U.S.-based organizations. This survey was limited to organizations with more than 500 networked users, and was selected non-randomly (for example, the researchers only invited organizations that they already believed to have suffered at least one cyber attack, and approximately half of the sample consisted of members of the Ponemon Institute's benchmarking community). PONEMON INST., 2013 COST OF CYBER CRIME STUDY: UNITED STATES 27 (2013), *available at* http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf?vm=r.

91. CTR. FOR STRATEGIC & INT'L STUDIES, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 4 (2013), *available at* http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf. While the study authors felt that the range of possible values was between $24 billion to $120 billion, $100 was their best guess within that range. It is also worth noting that this number does not reflect all of the damage to all victims. As it focuses only on net loss to the U.S. in general, a denial of service attack that costs company a sale does not create a loss if the customer goes on to purchase the product from company B (as, to the economy in general, it is irrelevant which business sold the item).

92. *See*, VERIZON, *supra* note 88, at 5–6.

rate at 2.0%. With this being said, merchants reject international orders nearly three times more than domestic orders (7.3% vs. 2.8%).[93]

The 2012 Norton Cybercrime Report gives statistics relating to twenty-four countries. This report indicates that the global price tag of consumer cybercrime is $110 billion U.S. dollars annually, with 556 million victims per year. According to the report, two-thirds of online adults have been victims of cybercrime in their lifetime. The top cybercrime reported was Internet fraud with 42% overall. The United States alone loses $21 billion annually due to cybercrime, second to China who loses $46 billion.[94]

NW3C's own research is in agreement with the trends illustrated by these isolated data points. In 2001, NW3C's Internet Crime Complaint Center (IC3) received 49,711 individual crime complaints; within ten years, the number of complaints had increased over 600%.[95] In the Internet Crime Complaint Center's 2012 Annual Report, 39.64% (114,908) of 289,874 complaints reported some sort of loss involving Internet fraud. This came to a total loss of $525,441,110.00 with an average dollar loss for those reporting loss of $1,813.[96]

a. Common Concerns

Computers and the Internet have opened up an entirely new realm of possibilities for the commission of white collar crime. The ability to reach literally millions of potential victims has magnified the potential financial reward for the criminal using the Internet as their means to commit crimes. The following list is by no means intended to represent all of the possible ways in which the computer and the Internet can be used to scam unwitting victims out of their money.

Internet fraud refers to criminal activities that utilize the Internet to commit a fraud or perpetrate some form of scam resulting in monetary loss to the victim. These crimes often encompass overlapping activities (such as a phishing scam that uses copyright and trademark violations to conduct identity theft during the commission of a fraud). Many frauds that migrate to the Internet have existed in one form or another for years, but have also evolved with technology. With almost 2.5 billion Internet users worldwide, of which over 270 million are in

93. CYBERSOURCE, 2012 ONLINE FRAUD REPORT 10 (2012).

94. NORTON, 2012 NORTON CYBERCRIME REPORT 7 (2012), *available at* http://now-static.norton.com/now/en/pu/images/ Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

95. NAT'L WHITE COLLAR CRIME CTR., IFCC 2001 INTERNET FRAUD REPORT (2002), *available at* http://www.ic3.gov/media/annualreport/2001_IFCCReport.pdf; NAT'L WHITE COLLAR CRIME CTR., *IC3 2010 Internet Crime Report* 5 (2011), *available at* http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf (referencing a figure of 303,809 reports).

96. NAT'L WHITE COLLAR CRIME CTR., IC3 2012 INTERNET CRIME REPORT 5 (2012), *available at* http://www.nw3c.org/docs/ic3-annual-reports/2012-internet-crime-report.pdf?sfvrsn=5.

North America,[97] potential fraud victims are just a keystroke away from criminals.

The Internet is an appealing medium for committing crime because it allows anonymous contact with a large pool of victims without incurring significant costs. Internet frauds of all types frequently rely on some of the same basic tools. Some of these tools are:

Phishing: Among other techniques, criminals can attempt to mimic ("spoof") legitimate websites and e-mail, in an effort to trick consumers into revealing sensitive information by interacting with them as if they had originated with the trusted party. The more detailed or realistic an online communication appears, the more likely a person is to accept the information conveyed as being valid or originating from a legitimate source. The victimization rate that results is usually somewhere in the 0.5% to 1% range.[98] However, when a phishing email can be sent to several thousand addresses with little investment of either money or time, that is more than enough of a return to make the enterprise profitable. In 2012, there were nearly 33,000 phishing attacks globally each month, which totaled a loss of $687 million. These phishing attacks mark a 19% increase globally compared to the first half of 2011.[99] It is estimated that 1 in 414 emails is a phishing attempt.[100]

Social Engineering: Many schemes also rely on social engineering, bypassing technological security measures by manipulating legitimate users into voluntarily divulging confidential information. A recent example of this technique occurred as a contest at the 2011 Defcon Conference. Several security professionals, in an effort to demonstrate the dangers of social engineering, called a number of software, telecommunications, and security companies and attempted to obtain information through social engineering. This included posing as IT professionals, calling employees, and simply asking them for sensitive data (such as login credentials). Many of the employees were helpful and compliant. [101]

Malware: Malware (malicious software) refers to any sort of computer program that is designed to perform functions that are against the interest of the person running the program. Because of the undesirable nature of the programs, they are typically delivered to end users surreptitiously and hide their activities (and, in most cases, their existence) on the target system. Malware may be delivered to end users disguised as other files, hidden within other files, or through hidden

97. *World Internet Users and Population Stats.*, INTERNET WORLD STATS (June 30, 2012), http://www.internetworldstats.com/stats.htm.

98. John Leyden, *One in 200 success rate keeps phishing economy ticking over*, REGISTER (Dec. 7, 2009), http://www.theregister.co.uk/2009/12/07/phishing_hit_rate.

99. *Phishing in Season: A Look at Online Fraud in 2012*, RSA (2012), http://blogs.rsa.com/phishing-in-season-a-look-at-online-fraud-in-2012/.

100. SYMANTIC CORP., 2013 INTERNET SECURITY THREAT REPORT, VOLUME 18, at 11 (2013), *available at* http://www.symantec.com/security_response/publications/threatreport.jsp.

101. Stuart Sumner, *Oracle Data Obtained in Social Engineering Attack*, COMPUTING (Aug. 9, 2011), http://www.computing.co.uk/ctg/news/2100282/oracle-obtained-social-engineering-attack.

downloads. All forms of electronic communication are possible vectors for malware distribution. It is estimated that 1 in 291 emails contains a virus (which is a type of malware).[102]

While there is very little risk of contracting malware from any established, reputable site, there are various tricks that criminals can use to entice users to leave a safe environment without realizing it. For example, a malware attack may be able to take place after a user clicks a link (possibly within a comment or user-generated post) that takes them offsite.[103] One interesting technique criminals use to trick users into installing malware is creating fake pop-up screens that look like the update screens used by various common web browser plug-ins (such as Adobe Flashplayer), in hopes that users (who will have routinely updated these products in the past as part of maintaining their browser software) will click on it without much thought. [104] Another technique involves attackers hacking into legitimate websites and adding malicious content that generates links to pages on an attack site. When unsuspecting users visit the legitimate site, their browsers also automatically pull down the exploit kit code from the malicious server.[105] 821,379,647 attacks from malicious websites were detected in Q1 of 2013.[106]

One significant permutation of "typical" malware activity is the botnet. Botnets are networks of computers that can work together to perform tasks. In this context, we are referring to criminal botnets – infected "zombie computers" that have been secretly linked together by malware and which are now invisibly controlled by third parties. It is estimated that 3.4 million computers are unknowingly slaved into botnets.[107] Botnets are available for rent. Prices range from 2 cents per computer (for a mix of 10,000 computers from around the world) to 10 cents per computer (for 10,000 American computers).[108]

b. Jurisdiction

Jurisdiction is an issue that can severely complicate investigations of online criminality. Internet investigations often pose unusual questions for the investigator. Chief among these inquiries is, "Where is the activity occurring?" In the online environment, the location of an activ-

102. *See* SYMANTIC CORP. *supra* note 100, at 11.

103. *Can you get a virus from Facebook?*, THATSNONSENSE.COM (Feb. 28, 2012), http://thatsnonsense. com/blog/can-you-get-a-virus-from-facebook/.

104. *Id.*

105. *Security Threat Report 2013*, SOPHOS 7 (2013), http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx.

106. Denis Maslennikov, *IT Threat Evolution: Q1 2013*, KASPERSKY LABS: SECURELIST (2012), http://www.securelist.com/en/analysis/204792292/IT_Threat_Evolution_Q1_2013.

107. *See* Symantic Corp. *supra* note 100, at 12.

108. Dancho Danchev, *How much does it cost to buy 10,000 U.S.-based malware-infected hosts?*, WEBROOT (Feb. 28, 2013), http://blog.webroot.com/2013/02/28/how-much-does-it-cost-to-buy-10000-u-s-based-malware-infected-hosts/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WebrootThreatBlog+%28Webroot+Threat+Blog%29.

ity is often more ambiguous than it would be in a real-world scenario. When residents of one state encounter a website that they believe to be illegal, has the website traveled to the state or have the citizens traveled to the website? Depending on the nature of the website (such as sites that might violate anti-gambling laws in some states but not in others), the answer to this question might directly impact whether a criminal act has occurred. Even when a clear consensus exists as to an action's illegality, however, the question of "where" the offense has occurred remains highly pertinent. While a law enforcement agency's mandate may give wide investigatory powers, the cases will eventually end up in court and the court may not have jurisdiction to hear the case if the acts in question occurred outside of its jurisdiction.

For federal investigators, much of this problem is already solved. Section 3237 of Title 18 of the U.S. Code authorizes the investigation and prosecution of federal offences in any district in which they were begun, continued, or completed. Further, the code section, when applied to offenses involving transportation in interstate or foreign commerce, allows investigation and prosecution in any district from, through, or into which such commerce moves. This allows two different supports for extending jurisdiction of the district court to an out-of-district defendant—that commerce moved through the district or that the offense was in some way continued or completed within it. For this reason, many investigations of online criminality are referred to federal law enforcement whenever possible.

For state and local investigators, establishing jurisdiction involves a more complicated analysis. States can only extend their legal powers outside of their own borders under limited conditions bound by due process and the state's long-arm statute.

Each state has some version of a long-arm statute, authorizing the state to apply its laws to out-of-state persons or events when certain conditions are met. These statutes vary from state to state, but one universal element is that, like any other state law, they have no ability to extend the state's power past the limits set by the U.S. Constitution. As a result, every long-arm analysis must also be a constitutional (and, hence, a due process) analysis. In most cases, state long-arm statutes are relatively clear and provide substantial latitude to law enforcement. While meaningful examination of the long-arm statutes in the several states is beyond the scope of this Article, understanding the constitutional restraints on the extraterritorial application of state power will, in most cases, serve to outline the majority of the framework governing a state's power over non-state residents.

The Fifth and Fourteenth Amendments guarantee that no one shall be deprived of life, liberty, or property without due process of law. Though the exact requirements of due process are debatable, one of the commonly understood requirements is that of notice. Under the requirement of notice, a state violates due process when it exercises its laws against someone who would have no reason to believe that they might be held accountable to the laws of that state.

Crucial to due process analysis, then, is the question of how courts determine if someone was on notice that they might be held accountable under the laws of a state. The modern method of determining when this requirement has been met is the "minimum contacts" test. As put forth by the Supreme Court, the notice requirement of due process is satisfied when the defendant has "certain minimum contacts with it such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[109]

The courts have implemented a three-prong test for determining when these minimum contacts have been met. The first prong is that the defendant must purposefully avail themselves of the privilege of conducting business in the forum. ("Conducting business" in this instance can also refer to non-commercial activity.) The second prong is that the cause of action must arise out of the defendant's activities in the forum. The third prong is that the exercise of jurisdiction must be fundamentally fair (which is a substantial subjective evaluation).

Physical presence and intentional targeting are relatively clear means of establishing "purposeful availment." An individual who drives through a state has purposefully availed themselves of the privilege of using the state's roads. A Ponzi scheme operator who mails invitations to participate to state residents has purposefully availed themselves of the privilege of contacting and conducting business transactions with residents of the state. When someone introduces objects or ideas into "the stream of interstate commerce," however, jurisdiction is more ambiguous. In a case involving online material that has been made available to the general U.S. public (without specifically targeting any particular state), the question becomes, when have they established minimum contacts with any of the states?

The Supreme Court has considered the matter of determining when minimum contacts have been established through items available in the stream of commerce. Unfortunately, their binding opinion on the situation was issued through a plurality, which means that there are two different tests for determining when minimum contacts have been met. Different jurisdictions may follow either test, but the prevailing test in most jurisdictions is the "something more" test.[110]

The "something more" test is whether the defendant did something extra to show that they knew and accepted the risk of being called into court in any particular state. U.S. Supreme Court Justice O'Connor gave a number of examples of activity that might count as "something more." These include indicating an intent to direct goods to the state, designing a product for the state's market, advertising in the state, selecting a distributor specifically for the state, and establishing channels for regularly advising residents of the state (such as local customer service numbers).

---

109. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

110. Asahi Metal Indus. Co. v. Super. Ct. of Cal., Solano Cnty., 480 U.S. 102, 111 (1987).

Applying this test to the Internet, the first question is whether the content is available to the general public of more than one state (and is therefore "in the stream of interstate commerce"). Most websites fall into this category, whereas private email does not. If it is within the stream of commerce, the next task is to see if "something more" can be found. Generally, a defendant who posts something online, without more, has not done enough to be prosecuted in any state court but their own. Posting child pornography, for example, violates federal law and a federal law enforcement officer can prosecute the offense in whichever federal district the officer's in (assuming that the images were transmitted there). A state law enforcement officer trying to use state law to act on the same image, however, will have trouble showing that the defendant purposefully availed themselves of the officer's state without some other element showing a willing connection to the forum (unless the defendant and the officer are in the same state).

When attempting to satisfy the "something more" requirement with Internet content, the first thing to look for is commerce. Is this a pay site? If a website allows customers to place orders that the owner then fills, it is directing goods to the state, and due process is satisfied. In the current hyperlinked environment, this bears a second look, however. If a website advertises a product but, when the "purchase" link is clicked on, actually routes the visitor to a distributor, the company may not actually be the one directing goods to the state. Simply advertising a product, even when the advertisement reaches a state, is not generally considered to be enough to constitute minimum contacts. As at least one court has found, it may be more difficult to prove purposeful availment with an Internet advertisement than a national print advertisement. While an advertiser can decide not to put an advertisement in a magazine that is distributed to a particular area, once a resource is on the Internet, the option of bypassing certain regions is not generally available.

c. Types of Internet Fraud

There are various types of Internet fraud ranging from the targeting of multiple victims with a "419" fraud (a.k.a. the Nigerian Scam),[111] as well as deceptive websites that procure money for non-existent charities. For practical purposes, the specific type of fraud committed should address Internet fraud. The most frequently reported (to IC3) types of Internet fraud include:

Auction Fraud

The Internet Crime Complaint Center defines auction fraud as "fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products

111. Barbara Mikkelson, *Nigerian Scam*, SNOPES, http://www.snopes.com/fraud/advancefee/nigeria.asp (last updated Feb. 1, 2010).

purchased through an Internet auction site."[112] Online shoppers visit auction websites to buy and sell various items in an online format that resembles a real-life auction. Prospective buyers can bid on almost any item imaginable, such as virtual property, antique merchandise, or a cheese sandwich. Upon winning, the victim sends payment for the auction item. The most popular and well known auction site is eBay. Others include WebStore, eBid, and Overstock.[113] The fraud occurs when the victim does not receive the item or receives an item of lesser value than advertised. Resolving a questionable transaction can be difficult, as the victim frequently has little information on the seller other than an e-mail address. Attempts to reach the seller may be ignored or delayed with lengthy excuses designed to delay resolution.

Auction scams can come in many different shapes and forms:

Triangulation, one of the newest and more complex auction fraud scams, can impact three victims at one time. A thief first steals a credit card number from the first victim. The thief finds a high-value item for sale on a site such as Amazon.com and posts it for sale on an online auction site for a cheaper cost. The winning bidder pays the scammer for the item. Meanwhile, the thief will purchase the item on Amazon .com with the stolen credit card and ship it to the winning bidder. When the credit card victim is aware of the charge, he cancels this transaction and the bank contacts Amazon.com and reverses the purchase. Amazon.com will then contact the online auction bidder and force him to surrender the item to them for non-payment even though the bidder thought he bought the item legitimately. This is an example of triangulation of three victims: the credit card victim, the auction site itself, in this example, Amazon.com, and the online auction bidder who ends up never being able to get his money back. [114]

Hidden Charges happen when the seller adds additional charges for postage and shipping and handling of the product. The buyer then ends up paying more than anticipated. Instead of having a flat rate on the shipping and handling like most companies, these hidden charges are often not seen by the buyer when initially purchasing the item.[115]

Fake bidding occurs when the seller bids on their item in an attempt to inflate the price.[116] This can also occur when a fake buyer submits higher bids to discourage other buyers from competing with an item; this type of bidding is called bid shielding.

In bid shielding, one person places a low bid while the other puts in an outrageously high bid, scaring other bidders away. In the final moments of bidding, the higher bidder will withdraw his bid, leaving

112. *Internet Crime Schemes: Auction Fraud*, INTERNET CRIME COMPLAINT CENTER, http://www.ic3.gov/crimeschemes.aspx (last visited March 13, 2013).

113. *2014 Online Auction Sites Comparisons*, ONLINE AUCTION SITES, http://online-auction-sites.toptenreviews.com/ (last visited Apr. 27, 2014).

114. *Triangulation, the Latest eBay Auction Fraud*, DOIT DIVISION OF INFORMATION TECHNOLOGY (Aug. 30, 2012), http://www.doit.wisc.edu/news/story.aspx?filename=1770.

115. *Online Auction Fraud*, NATIONAL CRIME PREVENTION COUNCIL, http://www.ncpc.org/cms-upload/ncpc/File/aucfraud.pdf (last visited Apr. 27, 2014).

116. *Id.*

the low bid as the best bidder. Sellers may never know why their products sold for such a low price. Some auction sites do not allow the withdrawal of bids so that this type of scam cannot happen, eBay, however, does allow withdrawal for legitimate reasons.[117]

The 2010 IC3 Annual Report mentions that, historically, auction fraud has been the number one complaint reported each year (with a high of 71.2% of referrals in 2004). In 2010, however, auction fraud only represented a little more than 10% of referrals. It is unclear whether this reflects the criminal element more fully exploiting the potential of a more diverse group of possible criminal uses for the Internet (the rest of the internet becoming less safe), an increase in the safety of internet auctions (auctions becoming more safe), or simply the increase of the use of IC3 as a reporting mechanism in wider variety of contexts.[118]

Non-Delivery of Merchandise or Services

Various fraudulent online schemes induce victims to send payment for merchandise and then deliver nothing in return or an item of far less value than expected. The same non-delivery occurs with services, when the merchant delivers a service but is never paid by the recipient. Services that request payments in advance, such as travel fees or moving costs, can also be involved in these sorts of crimes. In that variant, the customer pays and the perpetrator never renders the service. Both consumers and merchants can be victims of non-delivery in online frauds.

Business Opportunity Schemes

The key word in this type of fraud is opportunity. The prospect of getting rich quickly is the lure that draws many victims to business opportunity scams. Falling for these scams could also compromise the victim's own identity or personal accounts and implicate them in fraudulent check scams.[119] Another scheme involves an Internet-based business opportunity to use your home computer to earn money. Spam e-mails also allow criminals to batch out thousands of various money-making opportunities. Often, the information and tools provided for alleged success in business opportunity schemes are either fraudulent in nature or of minimal value. Business opportunity schemes also classified as employment scams that were reported to the Internet Crime Complaint center in 2011 showed losses of more than $20 million, with an average loss of $1,160 per complaint made.[120]

117. *eBay Sellers Face 'Bid Shield' Scam*, MSNBC (July 26, 2012), http://mars.superlink.net/~jason/ebay/msnbc_ebayfraud.html.

118. INTERNET CRIME COMPLAINT CTR., 2010 INTERNET CRIME REPORT: INTERNET CRIME TRENDS, *available at* http://www.nw3c.org/docs/ic3-annual-reports/2010-ic3-internet-crime-report.pdf?sfvrsn=3.

119. *Internet Crime Complaint Center's Scam Alerts*, INTERNET CRIME COMPLAINT CTR. (Sept. 19, 2012), http://www.ic3.gov/media/2012/120919.aspx.

120. INTERNET CRIME COMPLAINT CTR, s*upra* note 118.

Scareware/Ransomware Scams

Scareware seeks to extort money from consumers by intimidating them with false claims, then offering to sell them software that will rid their computer of the malware that was supposedly found on their machines. Ransomware causes the user's computer to freeze and offers to return access for a fee. One prominent type of ransomware, a program named Reveton, causes a warning to appear on their screen stating that the user has committed a violation of the law. The program displays a message that [whichever law enforcement agency would be appropriate for the localized version of the ransomware] has detected that the user's IP address has visited websites containing child pornography (or other illegal content) and the user is instructed to pay a fine using a prepaid money card service to unlock their computer and avoid future prosecution. The victim is provided with detailed instructions on how to procure the prepaid money card and enter the required information into their computer. In the process, the perpetrator often obtains identifying information from the victim to commit identity theft. According to the IC3, almost 2,000 complaints of this type of fraud were committed in 2012 with losses totaling $134,899.85[121]

Identity Theft

According to the Internet Crime Complaint Center, identity theft is any "unauthorized use of a victim's personal identifying information to commit fraud or other crimes."[122] Identity theft was the second most reported crime in 2011 according to IC3. This is a serious crime that can affect finances, credit score and history, and a victim's reputation. Resolving an identity theft attack can take time, money, and patience. Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Once an identity theft victim discovers that their information has been stolen, they may spend years cleaning up their credit history as well as monitoring their credit report for additional occurrences.

- The 2011 Internet Crime Report from the Internet Crime Complaint Center (IC3) reported that identity theft was the second highest complaint in 2011. Of the top five reported crime types, identity theft accounted for almost 22% of complaints.[123]
- In February of 2013, the Federal Trade Commission released its list of top ten complaint categories of 2012. In that list, Identity theft rated the number one complaint for the 13th consecutive year.[124]

121. NAT'L WHITE COLLAR CRIME CTR., *supra* note 96, at 13.

122. INTERNET CRIME COMPLAINT CTR., *2011 Internet Crime Report* 10 (2011), *available at* http://www. nw3c.org/docs/ic3-annual-reports/2011-ic3-internet-crime-report.pdf?sfvrsn=4.

123. *Id.*

124. *FTC Releases Top 10 Complaint Categories for 2012: Identity Theft Top List for 13th Consecutive Year in Report of National Consumer Complaints*, FED. TRADE COMM'N (Feb. 26, 2013), http://ftc.gov/opa/ 2013/02/sentineltop.shtm.

- In February of 2013, the Federal Trade Commission released its list of top ten complaint categories of 2012. In that list, Identity theft rated the number one complaint for the thirteenth consecutive year.[125]
- The identity theft survey by Javelin Strategy and Research, released in 2012, revealed that identity fraud had increased by 12.6% in 2011, suggesting that 11.6 million Americans were ID theft victims in 2011. Despite this increase, the annual overall fraud amount was at a relative low of $18 billion. Only about a third (35%) of victims made any sort of report to the police.[126]
- The average number of identities exposed per data breach is 604,826.[127]
- 24 million identities were stolen in the Zapos data breach (Jan 1, 2012)[128]
- 15% of American consumers have been notified that their information was compromised.[129]
- Consumers whose information has been compromised in a data breach are 9.5 times more likely to have the information misused.[130]
  - Of those whose compromised information was misused:
    - 41% saw their information used to make purchases online[131]
    - 35% saw their information used to make purchases in person[132]
    - 17% saw their information used to make purchases over the phone or through the mail[133]

Credit Card Fraud

Credit card fraud committed online is a multi-faceted crime. Initially, criminals use stolen or forged credit card numbers to purchase items from websites. Upon receipt of payment, the merchant ships the merchandise to the suspect. Upon discovery that the credit card number has been used illegally, the credit card issuer initiates a "chargeback" against the merchant. Since the merchant has already shipped the merchandise, they are left without the merchandise and without payment. The owner of the credit card must dispute the purchases with the credit card issuer and resolve any resultant credit

125. *Id.*

126. JAVELIN STRATEGY & RESEARCH, 2012 IDENTITY FRAUD REPORT: PARTNERING WITH LAW ENFORCEMENT (2012), *available at* http://itsecurity.und.edu/2012%20Identity%20Fraud%20Law%20Enforcement%20Report.pdf?vm=r.

127. SYMANTEC CORP., *supra* note 100.

128. *Id.*

129. LEXISNEXIS, LEXISNEXIS 2012 TRUE COST OF FRAUD (2012), *available at* http://images.solutions.lexisnexis.com/Web/LexisNexis/2012_LexisNexis_True_Cost_of_Fraud_Study.pdf.

130. *Id.*

131. *Id.*

132. *Id.*

133. *Id.*

issues on their credit report. In many credit card fraud cases, there are actually multiple victims: the website merchant, the card-holder, and the card issuer. All who are affected must spend time and/or money resolving the fraudulent issue. There is also the additional crime that was committed in obtaining or stealing the credit card number in the first place.

Credit card fraud represents 60% of all fraudulent transactions.[134] Over three percent of adult Americans were the victims of credit card fraud in 2011. [135] The average amount charged in those victimizations was $1,324.[136]

Online Investment Schemes/Securities Fraud

Stock market news and information that is posted in real-time on the Internet is often taken at face value by investors without additional research. Consequently, online investment schemes thrive when victims rush to take advantage of an opportunity with the hopes of making lots of money. One method that criminals use is the "pump and dump" scheme, through which stock information is disseminated via spam e-mail or Internet message boards in an effort to dramatically increase prices in thinly traded stocks. Once the price doubles or triples, the perpetrators sell off their holdings for significant profit margins. This scam leaves victims with lesser-valued stocks when the stock value falls. Conversely, the Internet can also be used to devalue stock with unfounded rumors or purposeful lies. The victims include both the stock holder and the company whose reputation is tarnished or even destroyed.

Romance Scams

In 2012, IC3 received over 4,476 complaints of romance scams in which scammers target individuals who search for companionship or romance online.[137] Victims of romance scams believe they are in a relationship with someone they feel is honest. What these victims do not know however is that their online lover uses the same script with other victims. Scammers use a variety of tactics such as flowers, love notes, or gifts to attract their victims. They express their "undying love" and tell victims stories of severe life tragedies and hardships to keep victims concerned and involved with their schemes. They entangle these victims in these love schemes and eventually ask them to send money to help with their tragedies and hardships. These scams take a toll on victims emotionally and financially. In 2012, victim reported losses to various romance scams totaled $55.9 million.[138]

134. *Id.*
135. *Id.*
136. *Id.*
137. INTERNET CRIME COMPLAINT CTR., 2012 INTERNET CRIME REPORT (2012), *available at* http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf.
138. *Id.*

Overpayment Fraud

The Internet Crime Complaint Center defines overpayment fraud as "an incident in which the complainant receives an invalid monetary instrument with instructions to deposit it in a bank account and send excess funds or a percentage of the deposited money back to the sender."[139] There are many variations of overpayment scams used by fraudsters. These scams often incorporate the use of fake checks. Scammers will offer to pay for an item with a check and write the check for more than the asked selling price. The scammer will then ask the victim to wire the difference back after they deposit the check. Later, when the check bounces, the victim is left liable for the entire amount and out the goods they were selling.[140]

III. Emerging Issues in White Collar Crime

A. *Criminal Use of Social Media*

The term "social media" refers to forms of online communication (generally, websites) wherein content is primarily user-created, the forum is geared towards sharing information with a large audience, membership in the user base is open to the general public, and in which the users are given some or all of the tasks of uploading, moderating, discussing, and modifying the content. Examples of social media include Facebook and Twitter.

Social media is extremely popular. Facebook claims to have 1.06 billion monthly active users.[141] Though it should be noted that, as the total number of Internet users worldwide is around 2.4 billion,[142] the number of user accounts may not be a one-to-one correlation with actual users. YouTube similarly claims 800 million users[143], and Twitter claims 500 million users.[144] In addition to personal usage, businesses and the public sector use social media to advertise, recruit new employees, offer better customer service, and maintain partnerships.[145] Social

139. Internet Crime Complaint Center, 2011 Internet Crime Report (2011), *available at* http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf.

140. *Fake Checks*, Federal Trade Commission (Dec. 2012), http://www.consumer.ftc.gov/articles/ 0159-fake-checks.

141. 1.06 billion user accounts are associated with activity involving Facebook or a Facebook-enabled app, program, or site each month. Facebook Inc. Form 10-K Annual Report (2013), *available at* http://investor.fb.com/secfiling.cfm?filingID=1326801-13-3.

142. *Internet Usage Statistics: The Internet Big Picture*, Internet World Stats (2012), http://www.internetworldstats.com/stats.htm?vm=r.

143. *Statistics*, YouTube, http://www.youtube.com/t/press_statistics (last visited Feb. 4, 2013). More than one billion unique visitors each month.

144. *Twitter Reaches Half a Billion Accounts More than 140 Millions in the U.S.*, Semiocast (July 30, 2012), http://semiocast.com/publications/2012_07_30_Twitter_reaches_half_a_billion_accounts_140m_in_the_US. 500 million user accounts.

145. Brian Anthony Hernandez, *5 Ways Businesses Will Use Social Media in 2011*, Business News Daily (Jan. 10, 2011), http://www.businessnewsdaily.com/five-ways-businesses-will-use-social-media-in-2011-0895/.

networking is the most popular online activity, accounting for 20% of time spent on PCs and 30% of mobile time.[146]

Almost three quarters (72%) of American Internet users are using social networking sites,[147] and this trend has not escaped the attention of the criminal element. Security experts have declared that social networks are "lucrative hot beds" for cyber scams, as criminals have moved onto these online communities along with the general population.[148]

By and large, the threats that exist on social media are the same threats that an internet user could encounter through any form of electronic communication. Con artists are still contacting users, tricking them into downloading malware, and compromising their accounts in ways that have changed little since the advent of email. What is different about these interactions is primarily that the social media sites contain a great deal more personal (and, in some cases, sensitive) information than earlier forms of electronic communication, and that this information is given far greater exposure to the public.

Another factor that makes predation on social media more troubling than predation occurring through other forms of electroinc communication is that the pool of potential victims continues to expand to include younger age groups. Roughly four out of five (81%) children aged 12-17 online are on social networking sites (compared to 67% of online adults). [149] These children are sharing more personal information on these sites than ever before:

146. NIELSEN, STATE OF THE MEDIA: THE SOCIAL MEDIA REPORT 2012, *available at* http://blog.nielsen. com/nielsenwire/social/2012/.

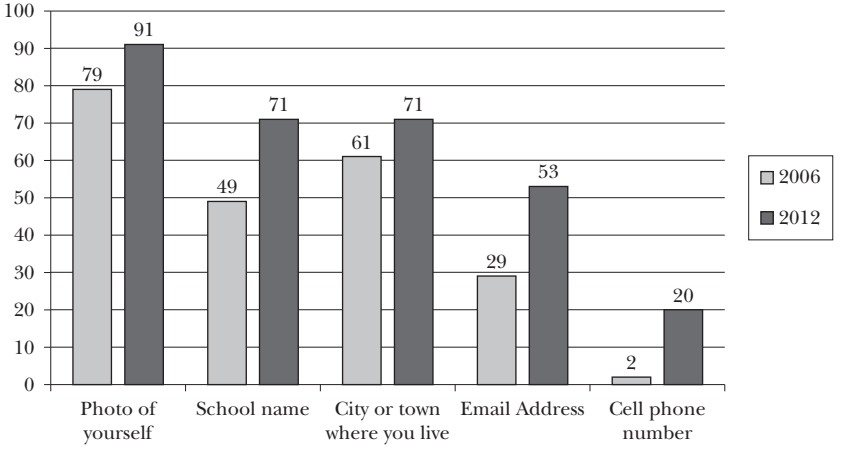
147. JOANNA BRENNER & AARON SMITH, PEWRESEARCHCENTER, 72% OF ONLINE ADULTS ARE SOCIAL NETWORKING SITE USERS (2013), *available at* http://pewinternet.org/~/media//Files/Reports/2013/PIP_Social _networking_sites_update.pdf.

148. Glenn Chapman, *Cyber Crime Rife on Social Networks: Microsoft*, AMERICAN FREE PRESS (May 12, 2011), http://www.google.com/hostednews/afp/article/ALeqM5io15Pj33QmaExnTQu7gsUxxND4GA?docId=CNG.a173e5b8fcaaae78675dd1b3e1b4a8c8.921.

149. MARY MADDEN ET AL., PEWRESEARCHCENTER, TEENS, SOCIAL MEDIA, AND PRIVACY (2013), *available at* http://pewinternet.org/~/media//Files/Reports/2013/PIP_TeensSocialMediaandPrivacy.pdf.

SOCIAL MEDIA PROFILES: WHAT TEENS POST — 2006 VS. 2012

Percent of teen social media users who say they post the following to the profile they use most often:[150]



B. *Privacy*

While privacy is hardly new as a concept, it has recently come to the fore of the national discussion.

Communications between individuals, regardless of the communications medium, may be anonymous (literally, without a name), pseudonymous (with a false name), or done in one's true name. There is some confusion, however, about how anonymous many online activities are.

True anonymity is something that is very difficult to achieve online. While one may browse web sites without affirmatively giving one's name, the underlying mechanisms involved in the process are creating and broadcasting a number of identities of their own. An Internet Service Provider (ISP) may know a user by the account under which they accessed it. A website may know a user by the Internet Protocol (IP) address that contacted it (an IP address that will resolve back to the ISP, who will be able to correlate it to the user account that they assigned it to at a particular time). An online advertiser may know the user by a unique code found in a small text file (or "cookie") that the user's browser silently and automatically downloaded in the background when their browser loaded the resources necessary to display the page that the user was visiting. Though most browsers can be instructed not to

150. Pew Internet Parent/Teen Privacy Survey, July 26–Sept 30, 2012. n=802 teens ages 12–17. Interviews were conducted in English and Spanish and on landline and cell phones. The margin of error for results based on teen social media users is +/- 5.1 percentage points. Comparison data for 2006 comes from the Pew Internet Parents & Teens Survey, Oct. 23–Nov. 19, 2006. n=487 teens with a profile online. The margin of error is +/- 5.2 percentage points.

accept cookies, the rest of these processes are automatic and inherent to the medium.

Most interactions online are pseudonymous: they are done under some name or identifier other than one's true name. This identifier might include a user name or Internet handle or, as described above, an IP address or cookie identifier. When users speak of being anonymous online, what they tend to mean is that the interactions *feel* anonymous, in that they do not feel like other parties to the communication have any way of knowing who they are (an assumption that is generally correct for most interactions). The distinction between feeling anonymous and actually being anonymous is important in that it informs much of the tension in modern privacy debate.

Though this discussion of privacy is far broader than the Fourth Amendment, the Reasonable Expectation of Privacy test is still illuminative, as it deals with the fundamental question of when an earnest expectation of privacy ought to be respected. The Supreme Court has ruled that a reasonable expectation of privacy exists when a) a person has a subjective expectation of privacy, and b) this expectation is one that society is prepared to recognize as reasonable.[151] It would seem that most users of the Internet exhibit subjective expectations of privacy. The main question, then, is whether that expectation is reasonable.

It is somewhat axiomatic that anything posted online has been intentionally exposed to the eyes of others and is, as such, no longer private.[152] Of interest to that discussion is the Third Party Doctrine, which holds that voluntarily revealing information to a third party for any reason voids the second prong. [153] Note, however, that there is some disagreement about how this applies to electronic communications. On the one hand, the Stored Communications Act was enacted

---

151. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). As the Court's opinion states, "The Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." There is a twofold requirement: first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

152. *Id.* at 351–52 (citations omitted). ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

153. United States v. Miller, 425 U.S. 435, 443 (1976) (citations omitted):

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

specifically to protect electronic communications and remote data because they lacked Fourth Amendment protections when not on the user's machine. Since being turned over to ISPs in-transit—as all information that reaches external networks must—would void their Fourth Amendment protections. [154] On the other hand, the Sixth Circuit extended Fourth Amendment protections to email, holding it to be analogous to a letter and an ISP analogous to a post office.[155]

What is less clear is the status of information that would not be evident to someone who viewed an isolated public posting. It is one thing to follow a car on a public street, and quite another to compile a log of every movement and interaction a person makes on public streets for six months. On this point the Supreme Court agrees, noting in the concurrence to Jones[156] that the ability to precisely record someone's

---

154. S. REP. NO. 99-541, at 3 (1986):
The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. *See* United States v. Miller, 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records). Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

155. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010):
If we accept that an email is analogous to a letter or a phone call, it is manifest that agents of the government cannot compel a commercial ISP to turn over the contents of an email without triggering the Fourth Amendment. An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient. Thus, the ISP is the functional equivalent of a post office or a telephone company. As we have discussed above, the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is. It only stands to reason that, if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception.

156. United States v. Jones, 132 S. Ct. 945, 955–56 (2012):
In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the Katz analysis will require particular attention. GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. *See, e.g., People v. Weaver*, 12 N.Y.3d 433, 441–442, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-

movements over months (with GPS tracking) potentially revealed so much sensitive data (including data that would tend to indicate religious and political affiliation, medical needs, and sexual orientation), that it exerted a potentially chilling effect on the freedoms essential to a free society. Further, the ability to store and mine that information for other purposes created a significant possibility of abuse.

This is almost exactly what is currently happening online. Every time you use a search engine, someone is logging your search interests. Every time you sign up for a credit card, you contribute information to a profile that includes your age, income level, education level, interests and hobbies, purchase preferences and a host of other information that you may not be aware you are revealing. Marketing experts prefer to claim that gathering this personal information is in the individual's best interest.

The term used in the industry is "Customer Relationship Management" (CRM)—"a comprehensive process of acquiring and retaining customers, with the help of business intelligence, to maximize the customer value to the organization." [157] In the process of engaging in this acquisition and retention effort, marketing agencies use what is referred to as 'data-mining techniques' defined as "widely used information technology for extracting marketing knowledge and further supporting marketing decisions. Market basket analysis, retail sales analysis, target market analysis, and cross-selling analysis are included."[158] Called "targeted marketing" in the industry, all of this information gathering is ostensibly intended to maximize profits for companies at the same time it is maximizing convenience for potential customers by predicting what they are likely to want. The latest trend to emerge is called "retargeting," or "when you look at an item in an

---

the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. *Pineda-Moreno*, 617 F.3d, at 1124 (opinion of Kozinski, C.J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois v. Lidster*, 540 U.S. 419, 426, 124 S.Ct. 885, 157 L.Ed.2d 843 (2004). [¶] Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).

157. E.W.T. Ngai et al., *Application of Data Mining Techniques in Customer Relationship Management: A Literature Review and Classification*, 36 EXPERT SYS. WITH APPLICATIONS 2592, 2592 (2009).

158. Chia-Cheng Shen & Huan-Ming Chuang, *A Study on the Application of Data Mining Techniques to Enhance Customer Lifetime Value*, 6 WSEAS TRANSACTIONS ON INFORMATION SCIENCE AND APPLICATIONS 319, 319 (2009).

online store and then an ad for that item follows you around to other sites." [159]

Problems can occur on two fronts. One is when those marketing agencies engage in what many see as overstepping the bounds of propriety by invading people's privacy. The other is when someone privy to one's information chooses to use the gathered information in legally impermissible ways (for example, identity theft).

1. Overstepping Bounds?

Some of these techniques are more controversial than others. For example, as recently as August of 2013, Google was sued by a group of non-Gmail users who sent emails to some of Gmail's 425 million users only to find out that Google scans emails sent through their system so the company can "target ads to users—a key component of the company's business model."[160] Those filing suit claim that this amounts to a violation of U.S. regulations prohibiting unauthorized wiretaps.

Even more disturbing to privacy advocates is the Google plan to link user data across its email, video, social-networking sites: Under the plan, information collected about individuals will be integrated across sixty Google products including Gmail, YouTube and web search. Users will have to agree to a new privacy policy that will encompass data including location measurements collected on mobile devices. The result is that Google will soon know more about who users are and what they do on the web, allowing it to target search results and advertising. Users will not be allowed to opt out of the changes, which took effect March 1, 2013.[161]

Google claims that their plan is for the good of the customer, the Google user, and will enhance their efficiency, productivity, personal convenience etc. "We can provide reminders that you're going to be late for a meeting based on your location, your calendar and an understanding of what the traffic is like that day, or ensure that our spelling suggestions, even for your friends' names, are accurate because you've typed them before."[162]

In April of 2010, the Secretary of Commerce formed an Internet Policy Task Force, which after much study, produced a set of recommendations concerning personal privacy and information gathering via the Internet. It recommends "the U.S. government articulate certain core privacy principles—in order to assure baseline consumer protec-

159. Joel Stein, *Data Mining: How Companies Now Know Everything About You*, TIME MAG. (Mar. 10, 2011), http://www.time.com/time/magazine/article/0,9171,2058205,00.html.

160. Ian Munroe, *Google Law Suit Stirs Debate over Email Privacy Rights*, CBC NEWS (Aug. 16, 2013), http://www.cbc.ca/news/technology/story/2013/08/15/gmail-privacy-lawsuit-google.html.

161. *Google Data Merge Called Privacy Threat*, CBC NEWS (Jan. 25, 2012), http://www.cbc.ca/news/technology/story/2012/01/25/tech-google-privacy.html.

162. *Updating our privacy policies and terms of service*, Google Official Blog, Jan. 24, 2012, http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

tions—and that, collectively, the government and stakeholders come together to address specific privacy issues as they arise."[163] The report supports the establishment of 'codes of conduct' that are "voluntary but enforceable rules" that sites agree to follow, with the FTC having the power to go enforce those rules.[164] In February of this year, Senator John D. Rockefeller IV introduced the "Do Not Track Online Act of 2013." In a statement by the new Federal Trade Commission Chairwoman Edith Ramirez delivered in April 2013, before the American Advertising Federation, the Commissioner noted "Consumers still await an effective and functioning do-not-track system, which is now long overdue."[165]

According to the L.A. Times, while the American Advertising Federation claims to support the concept of safeguarding the rights to privacy of Internet users there has been no voluntary movement toward compliance with the general recommendations of the Task force report of 2010. [166]

2. Identity Theft

A review of the number of major breaches of security in the Sophos 2013 annual report of hacked organizations shows some alarming findings:

> In 2013 alone, LinkedIn lost 6.5 million passwords, eHarmony 1.5 million, Formspring 420,000, Yahoo Voices 500,000, IEEE the world's largest professional association for the advancement of technology lost the user names and passwords of more than 100,000 unique users, all to hackers.[167]

The potential for exploitation of this personal information for identity theft is impossible to calculate, but is certainly vast. If the average cost of a data breach is (as some research suggests) $194 per record, [168] then we are potentially looking at something in the neighborhood of $1.7 billion in damages arising from the Sophos-identified incidents. While identity theft would doubtless continue to be a problem even without extensive corporate data-gathering, creating such complete profiles of consumers and keeping so many files in one place makes a tempting and lucrative target for identity thieves.

---

163. DEPT. OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY i (2010).

164. Id.

165. Jessica Guynn, *FTC Calls on Online Ad Industry to Agree on Do-Not-Track Standard,* L.A. TIMES (Apr. 17, 2013), http://articles.latimes.com/2013/apr/17/business/la-fi-tn-ftc-online-ad-industry-do-not-track-20130417.

166. *Id.*

167. SOPHOS, SECURITY THREAT REPORT 2013 11, *available at* http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf.

168. PONEMON INST., 2011 COST OF BREACH STUDY: GLOBAL 2, *available at* http://www.symantec .com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-global.en-us.pdf.

Conclusion

We realize that the discussion in this Article has covered a long list of topics. However, all of the issues discussed are in some material way, related directly to what most observers would call white collar crime.

The challenges of even defining the term white collar crime has eluded the academic and law enforcement communities for seventy-five years since it was first coined in 1939, and the debate continues to this day. Resolving this definitional debate is the first step in obtaining some realistic measure of the extent of the damage being done to our society by this area of criminal activity.

Complicating the task of defining white collar crime is its rapidly evolving nature. As computers and the Internet become more and more an integral part of everyday life, the ability to commit widespread financial crimes victimizing vast numbers of people and on a global basis, increases at an alarming rate. Further complicating the task is the way these same tools have changed the typical image of the white collar criminal from the highly placed executive heading a large company, a banker in a position to embezzle large amounts of cash or a politician with a political machine to assist in their illicit endeavors, to just about anyone with the computer skills and basic knowledge needed to engineer identity theft, hack into a computer system, perpetrate a mortgage fraud or traffic massive quantities of child porn on the Internet.

Along with the evolution of these electronic tools also comes a new and challenging field of determining exactly how to effectively investigate and prosecute these crimes. Law enforcement and prosecutorial personnel have to learn new skills in identifying, seizing and processing electronic and digital evidence. The ability to encrypt and hide potentially incriminating evidence is increasing the number of issues involving right to privacy, self incrimination, freedom of speech, etc., that the legal community will have to struggle with in the future and all while this evolving field of criminality is creating more financial damage and victimizing more people than arguably, any other area of crime in history.

Conclusions are almost impossible to draw, only inferences as to the immensity of the challenges for the future of law enforcement and the legal community in addressing this rapidly evolving and extremely challenging field of criminality.