Docket:	:	I.13-10-003
Exhibit Number	:	
Commissioner	:	C. Peterman
Admin. Law Judge	:	D. Burcham

CALIFORNIA PUBLIC UTILITIES COMMISSION
SAFETY AND ENFORCEMENT DIVISION

EXPERT WITNESS TESTIMONY OF LEE TIEN

- CORRECTED -

INVESTIGATION OF COMCAST PHONE OF CALIFORNIA, LLC AND RELATED ENTITIES CONCERNING THE UNAUTHORIZED DISCLOSURE AND PUBLICATION OF UNLISTED TELEPHONE NUMBERS

I.13-10-003

San Francisco, California
July 18, 2014

99088660

TABLE OF CONTENTS

I. QUALIFICATIONS

Q1: What are your qualifications to offer testimony here on the question of privacy?

A1: I have worked in the privacy field for 14 years. As a senior staff attorney at the Electronic Frontier Foundation, a San Francisco based non-profit public interest group, I work on a many privacy issues, including electronic health records, telecommunications privacy, biometrics, online behavioral advertising, identity management, national security surveillance, and location privacy. In particular, I have: worked on federal and state privacy bills; spoken (by invitation) at privacy panels and workshops of the Federal Trade Commission[1] and other government bodies, most recently the White House's "big data" workshop in Berkeley;[2] written law review articles about privacy.[3] I have been an active participant in this Commission's smart grid privacy proceeding (R.08-12-009). I also am part of a litigation team challenging the legality of surveillance by the National Security Agency (pending cases in the Northern District of California).

II. REVIEW OF FACTS RELATED TO THIS INVESTIGATION, AND SCOPE OF TESTIMONY

Q2: What have you done to familiarize yourself with the facts of this Investigation?

A2: I have reviewed the Commission's Order Instituting Investigation (I.13-10-003), customer complaints, and a few Comcast - internal documents. Unfortunately, there was a week delay in Comcast's approving my access to confidential documents (and it is my understanding that Comcast has labeled every document it produced in this case as "confidential"), so I was not able to review as much of the internal documentation as I would have liked. I have also reviewed filings in the case of *LSSi Data v. Comcast Phone LLC,* 785 F. Supp. 2d 1356 (N.D. Ga. 2011). Finally, I have had discussions with

[1] *See, e.g.,* FTC's Workshop on Internet of Things – Privacy and Security in a Connected World, at http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world (speaker bios).

[2] *Cf.* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf; video available at http://www.youtube.com/watch?v=tuxC4ZpFHEg.

[3] *See, e.g.,* Lee Tien, THINKPIECE: Architectural Regulation and the Evolution of Social Norms, 7 YALE JOURNAL OF LAW & TECHNOLOGY 1 (2004 / 2005).

the Commission's staff counsel. I also had discussions with experts in the privacy community about the facts as recited in the OII.

Q3: What is the scope of your testimony?

A3: I want to address different but related aspects of Comcast and the privacy issues around Comcast's unlisted and/or non-published services[4]: (1) what are the reasonable consumer expectations with regard to a non-published telephone number, and how are those reflected in law? (2) did Comcast meet its duty with regard to the privacy of its non-published customers? and (3) what is the role of telephone numbers and other subscriber information (names, addresses) in the world of big data and data marketing?

III. STARTING POINT – CONSUMER EXPECTATIONS & THE LAW.

Q4: What are consumer expectations of privacy, particularly where the consumer has asked for a non-published number, and were those expectations defeated here?

A4: Consumers have a reasonable expectation of privacy and/or anonymity in unlisted or non-published numbers—especially in California—and those expectations were defeated here by the open publication of the unlisted and non-published numbers of its customers.[5] By guarding the link between the information (one's phone number) and one's identity, name and address, a consumer can try to protect her privacy. California law protects the privacy of unlisted numbers in very specific ways. Under the state constitution, consumers have a reasonable expectation of privacy in their unlisted name, address, and telephone number.[6] As the California Supreme Court recognized in

---

[4] Although I am aware that unlisted or non-listed service suppresses a telephone number only for directory listing (DL) but not for directory assistance (DA), whereas non-published or unpublished suppresses the number in both services, I use the terms interchangeably here, as at root the privacy principles are the same in both cases. I note that the Order Instituting Investigation 13-10-003 (OII) uses the word "unlisted" to encompass both services.

[5] The consumer complaints set forth in the OII and Staff Report, and consumer declarations more recently gathered by CPUC staff (see Momoh Testimony, **Attachment P**), confirm that customers do in fact have the expectations described here.

[6] OII, at 14 fn. 70, citing *People v. Chapman* (1984) 36 Cal.3d 98, 108 ("by affirmatively requesting and paying an extra service charge to the telephone company to keep her unlisted information confidential, respondent took specific steps to ensure greater privacy than that afforded other telephone customers"); *see also State v. Butterworth*, 737 P.2d 1297, 1300 (Wash. Ct. App. 1987) (noting that individual "specifically requested privacy regarding his address and telephone number in asking for an unpublished

(continued on next page)

People v. Chapman, "an unlisted number is usually requested in order that a person's name and address will not be revealed to anyone other than the telephone company. The fact that a significant percentage of customers take affirmative steps to keep their names, addresses and telephone numbers confidential demonstrates the importance of this privacy interest to a large portion of the population.").[7]

The protection given unlisted numbers by P.U. Code § 2891.1(a) clearly reinforces the command of Article I of the California Constitution, § 13,[8] in the context of phone service providers.[9] The California Constitution, *Chapman,* and the Public Utilities Code establish the legitimacy of customers' privacy and anonymity expectations for the purposes of this proceeding. But the legal and social recognition of the privacy of unlisted numbers in California and the United States runs much deeper.

For instance, the Telecommunications Act of 1996 protects the privacy of call records in the hands of telephone companies.[10] A telephone company may not use, disclose, or permit access to Customer Proprietary Network Information (CPNI) without

---

(continued from previous page)
listing").

[7] *Id.* at 109.

[8] Article I, section 13, provides that: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable seizures and searches may not be violated; and a warrant may not issue except on probable cause, supported by oath or affirmation, particularly describing the place to be searched and the persons and things to be seized."

[9] *See also* P.U. Code § 2894.10(a) (purpose to "protect residential telephone subscriber's privacy rights with respect to telephone solicitations"). Also, private unlisted telephone numbers obtained by certain government emergency agencies under § 2891.1(c)(2)(A) are specifically exempt from disclosure under the state Public Records Act. Gov't Code § 6254(z).

[10] 47 U.S.C. § 222 (protecting "customer proprietary network information" (CPNI)).*See* 47 U.S.C. § 222(h)(1) (defining CPNI as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information.").

that customer's consent except to provide service or to comply with the law.[11] "Congress' primary purpose in enacting § 222 was concern for customer privacy."[12]

More recently, the Telephone Records and Privacy Protection Act (TRPPA), 18 U.S.C. § 1039, responded to the burgeoning market in consumers' phone records. Enacted in 2007, TRPPA generally makes it unlawful to sell or transfer or buy or receive "confidential phone records information"[13] of a telecommunications carrier or a provider of IP-enabled voice service, without prior authorization from the customer to whom such confidential phone records information relates. 18 U.S.C. §§ 1039(b)(1), (c)(1).[14] Notably, Congress found in TRPPA that "the unauthorized disclosure of telephone records not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations." *See* Pub. L. 109–476, § 2, Jan. 12, 2007, 120 Stat. 3568.

As TRPPA recognizes, the link between unlisted phone numbers or home addresses and personal privacy is especially significant for categories involving law enforcement and domestic violence. The California Secretary of State offers an online opt-out form that Safe at Home participants can use to remove their home address, telephone number or personal identifying information from a website.[15] The law also

---

[11] *See* 47 U.S.C. § 222(c)(1); 47 C.F.R Part 64, Subpart U (CPNI regulations).

[12] *U.S. West, Inc. v. F.C.C.*, 182 F.3d 1224, 1236 (10th Cir. 1999).

[13] The definition of "confidential phone records information" in 18 U.S.C. § 1039 is similar to the definition of CPNI. *See* 18 U.S.C. § 1039(h)(1) ("information that—(A) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer; (B) is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or (C) is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer.").

[14] The prohibitions of both 47 U.S.C. § 222 and TRPPA are subject to the statutory exemptions in 47 U.S.C. § 222(d). *See* 18 U.S.C. §§ 1039(b)(2), (c)(2).

[15] *See* http://www.sos.ca.gov/safeathome/.

prohibits a person, business, or association from knowingly and intentionally posting or displaying on the Internet, or soliciting, selling, or trading on the Internet a participant's home address, telephone number or personal identifying information and imposes a fine for violations of this law.[16]

Importantly, the legitimate and reasonable expectation of privacy and anonymity that unlisted phone customers enjoy is not solely based on the harm or risk, potential or actual, that may result from an unauthorized disclosure. That would be a far too grudging approach. California's general, fundamental constitutional right to privacy encompasses, but is not limited to, protection against such harms. In *White v. Davis*[17] the California Supreme Court explained that "the moving force" behind California's constitutional right to privacy "was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society," and that its "primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy."[18]

Importantly, our state constitutional privacy right protects Californians against private businesses as well as the government. As the *White* court put it, the right "prevents government and business interests from collecting and stockpiling unnecessary information about us," partly because "[t]he proliferation of government and business records over which we have no control limits our ability to control our personal lives."[19] Thus, among the "principal 'mischiefs'" targeted by the constitutional right are "the overbroad collection and retention of unnecessary personal information by government and business interests" and "the improper use of information properly obtained for a

[16] Gov't. Code §§ 6208.1, 6208.2.

[17] *White v. Davis*, 13 Cal.3d 757 (1975).

[18] *Id*. at 774.

[19] *Id*.

specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party."[20]

The Commission has recognized its constitutional obligations to protect privacy in past decisions. When confronted with the consumer privacy concerns presented by telephone monitoring technologies in Decision No. 88232, the Commission unequivocally stated that, "[o]ur constitutional responsibilities and those of the utilities we regulate, are paramount. . . ."[21] In *The Matter of the Application of Pacific Bell,* when confronted with the consumer privacy concerns presented by Pacific Bell's default installation of caller identification technology, the Commission stated:

> If the service is to be offered consistently with constitutional guarantees and the public interest, it must be offered in a way that maximizes the ease and freedom with which California citizens may choose not to disclose their calling party numbers. We will not compromise an individual's free exercise of his or her right of privacy in order to place in the hands of the Caller ID subscriber a more valuable mailing list, a marginally better method of screening or managing telephone calls, or even a slightly more effective deterrent to unlawful or abusive uses of the telephone.[22]

Comcast is in the communications business, and should have known all this. At a minimum, it should have known that consumers who pay a monthly fee to maintain the confidentiality of their phone numbers are far more likely to have specific reasons for confidentiality, such as concern about telemarketing calls, threats from ex-partners, and so on. Non-published customer complaints to Comcast confirm consumers' expectation of privacy.[23] For these individuals their phone numbers are more sensitive than for other people. An analogy to health information may be apt: while we all believe in patient-physician confidentiality, we treat certain kinds of health information—mental illness,

---

[20] *Id*. at 775.

[21] *In re PT&T Co.*, 83 C.P.U.C. 149 (1977).

[22] *In re Pacific Bell*, 44 C.P.U.C.2d 694 (1992).

[23] See generally, Testimony of Rahmon Momoh.

HIV status, alcohol and drug treatment, reproductive health—with special care. In paying for a non-published number, consumers rightly had the expectation that their data would be protected with special care.

IV. PROTECTING PRIVACY IS DIFFERENT THAN PROTECTING OTHER CONSUMER INTERESTS.

Q5: How is protecting privacy different than protecting other consumer interests, like reasonable rates or adequate service quality?

A5: Privacy is an area of special concern for a variety of reasons. Information disclosure problems are not like many other kinds of legal problems. If you buy a new telephone from a phone company but your phone doesn't work, you know that something went wrong and you can do something about it right away. If your rates are too high, or your bill contains unauthorized charges, you will know on receipt of the bill. But if your telephone company covertly sells your subscriber information, you won't know until much later (if at all) that this had been done.

Moreover, privacy breaches have always been hard to undo; no one can be forced to forget something they know. Digital technology has made the problem exponentially worse, because information – once posted to the Internet -- can spread around the globe in a matter of minutes. Finally, particularly in the Internet context, the "Streisand effect" has come to mean that attempts to vindicate one's privacy can often lead to more publicity.[24]

V. PRIVACY INTERESTS IN THIS CASE

Q6: How would you formulate a standard of care for this case?

A6: Given the fact that Comcast customers paid, and Comcast accepted, $1.50 every month to protect their [its customers'] privacy, I think that Comcast had both contractual and constitutional duties toward its non-listed and non-published customers. Especially given *Chapman* and § 2891.1, the simplest and most natural way for the Commission to conceptualize Comcast's duty of care is in terms of negligence *per se*, under which "the

[24] http://en.wikipedia.org/wiki/Streisand_effect.

conduct prescribed by the statute [operates] as the standard of care for a reasonable person in the circumstances."[25] Under negligence *per se*, the legal questions are whether the injury resulted from the kind of occurrence the statute was designed to prevent, and whether the plaintiff was one of the class of persons the statute was intended to protect.[26]

Q7: Did Comcast Meet its Duty of Care in this Case?

A7: I do not think so.

Here, it seems clear that the open publication of unlisted numbers is exactly the kind of occurrence that § 2891.1 was designed to prevent, and the Comcast customers who paid for unlisted numbers are precisely the class of persons that § 2891.1 was intended to protect. This approach seems consistent with the clear state constitutional policy of recognizing an expectation of privacy in unlisted phone numbers.

A. Before the Breach

Q8: Did Comcast Meet its Duty of Care Before Discovery of the Breach in October 2012?

A8: Based on the information available to me, the actions (or inaction) of Comcast in this proceeding clearly defeated many of its customers' privacy expectations. Not only did Comcast somehow publish information that it specifically agreed to keep confidential, Comcast apparently did not monitor its own paper or online directories well enough to realize that it had made this serious "process error" for more than two years, despite receiving many customer complaints about this breach.

In other words, there are at least two distinct sets of factual issues here, neither of which is clear at this time: how Comcast caused more than 74,000 non-published or unlisted numbers to have been published at all; and how Comcast's precautionary or monitoring practices failed to alert it to the breach so that it could begin to mitigate the damage to its customers.

---

[25] *Casey v. Russell* (1982) 138 Cal.App.3d 379, 383.

[26] *Jacobs Farm/Del Cabo, Inc. v. Western Farm Service, Inc.* (2010) 190 Cal.App.4th 1502, 1526.

For instance, evidence strongly indicates that:

- Non-published/unlisted numbers began to appear as published in 2009, if not earlier;
- Non-published/unlisted numbers appeared on Ecolisting.com beginning in July 2010;
- Comcast did not formally discover the Ecolisting publication until October 2012; and
- Consumer complaints about these incidents began as early as 2009.

Q9: Has Comcast made attempts to limit its "privacy" duties among its customers?

A9: Yes, apparently. While Comcast's "Welcome Kit" says that it "ensures" a non-published number, Comcast's Privacy Notice suggests that Comcast takes a "best efforts" approach to non-published numbers.

> We take reasonable precautions to ensure that non-published and unlisted numbers are not included in our telephone directories or directory assistance services, but we cannot guarantee that errors will never occur.[27]

Given the clear state policy above, it makes little sense to think that Comcast could qualify its duty of care by using a best efforts provision. Even viewed as a matter of pure contract law, the purpose of Comcast's promise to keep confidential phone numbers out of directory assistance and out of phone directories and online directories was clearly to achieve a result: privacy. That purpose failed.

Admittedly, it remains unclear exactly how the non-published numbers somehow became published numbers. But here a related tort doctrine, *res ipsa loquitur,* provides the conceptual framework. This doctrine "is applicable where the accident is of such a

[27] Comcast's Privacy Notice is available online at http://cdn.comcast.com/~/Media/Files/Legal/CustomerPrivacy/CustomerPrivacy.pdf?vs=3, and it is discussed in the Testimony of Commission staff witness Nathan Christo (and is found there as Attachment A).

nature that it can be said, in the light of past experience, that it probably was the result of negligence by someone and that the defendant is probably the one responsible."[28]

On the information available at this time, Comcast did not meet its duty of care.

B. After the Breach But Before Its Discovery

Q10: What about Comcast's actions after the data breach, but before its discovery?

A10: I am very concerned about Comcast's actions after the data breach. As noted elsewhere in my testimony, any reasonable telephone provider in California should have been aware of the strongly protected, well-settled expectation of privacy that customers have in their non-published numbers. The record available to me, however, strongly suggests that Comcast did not have good mechanisms, policies or procedures in place that could address processing errors leading to the publication of non-published numbers.

For instance, Comcast apparently has concluded that the processing error occurred in June 2010, but that the discovery of the breach did not occur until October 2012. "It took Comcast 27 Months to Detect the Unauthorized Disclosure and Publication of Unlisted Telephone Numbers,"[29] even though Comcast had received customer complaints about this problem as early as March 2010, if not earlier.[30]

This delay in discovery compares poorly to the ten-month delay in an earlier case, where software used by Cox "began failing to place a 'customer privacy designator' on the names of Cox customers who had requested unlisted or unpublished listings" in August 1999.[31] Cox was not aware of the problem until May 4, 2000, when it *began* to receive complaints about new directories that Pacific Bell was distributing.[32] Cox

---

[28] *Howe v. Seven Forty Two Co., Inc*. (2010) 189 Cal.App.4th 1155, 1161; *see Brown v. Poway Unified School Dist.* (1993) 4 Cal.4th 820, 825–826.

[29] OII, at 7.

[30] Id. at 9.

[31] Interim Decision Relieving Pacific Bell Telephone Company and Cox California Telcom., L.L.C. of Obligation to Undertake Additional Measures to Reclaim Tainted San Diego Directories, at 4, Decision 01-11-062 (Nov. 29, 2001).

[32] *Id.,* Slip Op. at 4. ("Cox apparently did not become aware of this problem until May 4, 2000, when it began receiving calls from San Diego customers who had requested unlisted or non-published numbers but whose names and numbers appeared in the new directories that Pacific was distributing. ").

quickly "connected the dots" between in-bound complaints, and its directory listing duties, and did so apparently as soon as the complaints started.

C. After Discovery of the Breach

Q11: What about Comcast's actions after discovering the breach in October 2012?

A11: This period also reflects a certain casualness on Comcast's part about the privacy breach and its ramifications for the lives of its customers. It took Comcast three months from the mid-October discovery date to reach outside the confines of its corporate agency agreement with Targus, and contact the Commission and consumers, for a breach affecting approximately 75,000 customers.[33] By contrast, Cox contacted Pacific Bell (who was, by all appearances, not acting as Cox's agent) the day after discovering it had a problem,[34] and demanded the immediate halt to distribution and the claw-back of already distributed directories; within a month, Cox brought the matter to the Commission's attention with a motion to compel Pacific's action in this regard;[35] The number of affected customers was 10,778.[36]

Moreover, Comcast's responses to consumer post-notification complaints, as set forth in the OII, do not appear to be satisfactory.[37] In the case involving Cox and Pacific, Cox not only discovered the breach more quickly than Comcast, but also made an across-the-board offer to mitigate the damage to customers whose numbers had been erroneously published, including a choice between free changes to a new unlisted number (with 120 prepaid minutes), and retaining one's old number with a one-year package of free services to help screen unwanted calls. Moreover, Cox offered "escalation procedures" for customers with special safety concerns, such as judges, correctional officers, and those who had received specific threats from a specific person in the past.[38]

---

[33] OII, at 2-3.

[34] D.01-11-062 at 4. ("Both parties agree that Cox informed Pacific of the problem the next day").

[35] D.01-11-062 at 4.

[36] Id. at 27.

[37] OII at 10-11.

[38] D.01-11-062, at 8.

As another data point, in 2009, "[a]s a result of a 'feed error' from IT, Verizon inadvertently sent approximately 12,400 non-list/non pub listings" to "an unaffiliated directory publisher."[39] Verizon offered a package similar to that offered by Cox.

All of these cases involve some kind of information technology error, as appears to be the case with the Comcast breach. The Comcast breach affected many more customers, and involved Internet publication in addition to "tainted directories." Indeed, the fact that the Comcast breach occurred in a digital/Internet environment meant that the stakes (and dangers of immediate propagation) were much higher. Yet Comcast took much longer than Cox to discover the breach[40] in the first place, much longer to go public with the breach, and apparently offered its customers much less compensation for their loss of privacy. These factors strongly suggest that Comcast did not meet the expected level of company care, either in preventing and detecting the privacy breach, or in attempting to remedy the situation after it became known.

VI. THE VALUE OF SUBSCRIBER LIST INFORMATION TO DATA BROKERS, AND THE RISKS TO CONSUMERS FROM ITS EXPOSURE.

Q12: Is Comcast's Subscriber List Information Valuable, and Can Its Exposure Cause Harm?

A12: A consumer's phone number is a highly prized commodity in the data broker world. After a consumer's name and other information have been tied to a phone number, it can be sold repeatedly on data broker lists, where it becomes widely disseminated. Access to a consumers' phone is literally sold for a price, most typically expressed as a price per thousand names with phone numbers. Great consumer harm has come from phone number availability to data brokers.

[39] Maryland Public Service Commission, In the Matter of Verizon Maryland Inc.'s Disclosure of Certain Unpublished Subscriber Lists, Case No. 9176, Order No. 82668, at 1-2 (May 12, 2009).

[40] I do not presently have information about how long it took to detect the Verizon breach in Maryland.

Charles Guthrie, an elderly veteran, was bilked of his savings after he entered a sweepstakes and his name and phone number appeared on a marketing list. The list was sold by commercial data broker InfoUSA to a group of thieves, who then used the information to greatly harm him and other individuals. The story, which appeared in the New York Times, details the data trail of the veteran's information as it was sold to criminals and then used to defraud him.

> InfoUSA advertised lists of 'Elderly Opportunity Seekers,' 3.3 million older people 'looking for ways to make money,' and 'Suffering Seniors,' 4.7 million people with cancer or Alzheimer's disease. 'Oldies but Goodies' contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: 'These people are gullible. They want to believe that their luck can change.' As Mr. Guthrie sat home alone -- surrounded by his Purple Heart medal, photos of eight children and mementos of a wife who was buried nine years earlier -- the telephone rang day and night.[41]

For Mr. Guthrie, what began as a sweepstakes response ended with a real individual's phone number being sold on a list, which allowed him to be categorized and then sold to the highest bidder to be exploited. The phone was the medium that allowed repeated data broker sales of the information and repeated fraudulent contact of a vulnerable person.

Mr. Guthrie's case is not an isolated instance. Mr. Guthrie knew how his phone number was acquired. But Comcast customers who had their unpublished phone number sold to LSSi, a data broker, or displayed through Targus caller ID, or published in print directories, or published in an online directory without their permission or knowledge, would not have reason to know that third parties including companies ranging from data brokers to debt collectors to telemarketers could then grab their phone numbers and use them at will.

[41] Charles Duhigg, Bilking the Elderly with a Corporate Assist, New York Times, May 20, 2007. <http://www.nytimes.com/2007/05/20/business/20tele.html?_r=1>.

This problem is illustrated in the Declaration of Comcast customer Jane/John Doe 3, who indicates that they are in the senior range, and that they were hounded and harassed after Comcast repeatedly made their phone number visible to third parties:

> While it might be a bit of an exaggeration, I have remarked that the publication of our non-listed/non-published number has led to a "living hell." We now receive telemarketing calls at all times, beginning sometimes at 8.30 a.m. in the morning, and continuing through the day. At this point, I don't think Comcast's voicemail apologies to us are enough. (Declaration of John/Jane Doe 3).[42]

This is not surprising, given the scope of third party data brokering activity. A 2013 study of the data broker industry conducted by Harvard Business School Prof. John Deighton for the Direct Marketing Association found that the universe of data brokers numbered approximately 3,500 companies.[43] One of the external indicators of underlying activities comes from the publication of data brokers' "data cards," where data brokers list what data they are selling, for how much, and what the data sets include. Topics for data cards include consumer medical information, financial information, level of education, home ownership, number and ages of children, interest in certain activities, and many more categories.

One major site in this data bazaar is NextMark.com, which offers about 60,000 data cards advertising specific data broker lists that offer information for sale about everything from information about consumers with diseases to which consumers are in debt. Many data broker lists at NextMark (and elsewhere) are sold at a price for a quantum of phone number related data – the prized item for which data broker customers must pay (indicated on most listings in a variety of ways). Costs vary by the list, but in general, phone numbers are sold in price per thousand numbers attached to specific

[42] Found as Attachment P.3 to the Prepared Direct Testimony of Rahmon Momoh in this Investigation.

[43] Panel comments by John Deighton, National Press Club, The Value of Data: Consequences for Insight, Innovation and Efficiency in the US Economy; A Symposium Hosted by DMA's Data-Driven Marketing Institute, October 29, 2013. Dr. Deighton was commenting on his sampling for the study, The Value of Data: Consequences for Insight, Innovation and Efficiency in the U.S. Economy, John Deighton and Peter Johnson, DDMI, 2013.

consumer names and other information, such as a medical condition, credit scores, or other data pieces about the consumer.

A search for data broker lists on NextMark.com for lists that included seniors' phone numbers revealed 2,685 lists available on July 14, 2014. (This quantity changes as the availability of lists change.) List names included:

- Mature living seniors - Hispanic
- Senior shoppers from the Senior Source
- African American Senior citizens
- Senior Citizen donors
- Long life savings -- wealthy seniors

Regarding the scope of the phone numbers offered, a search on the same day for a list of consumers with illnesses offered more than15 million (15,624,050) phone numbers of consumers available for purchase.[44] One list of high net-worth seniors offered 571,800 phone numbers as available for purchase.[45] Another list of people with diabetes offered 401,320 phone numbers available for purchase.[46]

Seniors and other consumers who choose to make their phone numbers unavailable and unpublished often do so to stay off of telemarketing lists and other marketing activities that result from data broker dissemination. Given the scope of the dissemination of consumer phone numbers post-publication, this is wise.

Importantly, data broker lists and databases are used in ways that do not square with consumer expectations of privacy or of data use. For example, few consumers realize that disparate pieces of information gathered together and analyzed impact how much they will pay for their health plans. It is nevertheless true, and has been unambiguously demonstrated.[47] Consumers also do not generally know that data brokers

[44] (http://lists.nextmark.com/market?page=order/online/datacard&id=326525).

[45] (http://lists.nextmark.com/market?page=order/online/datacard&id=340749).

[46] (http://lists.nextmark.com/market?page=order/online/datacard&id=340272).

[47] See The Scoring of America, World Privacy Forum, p. 16, 17 <http://www.worldprivacyforum.org/wp-content/uploads/2014/04/WPF_Scoring_of_America_April2014_fs.pdf> and Satish Garla, Albert

(continued on next page)

desire phone numbers from consumers both to sell them outright, and also to use them as indexing and disambiguating tools.

Many people who are not aware of the details of data broker methods think that the Social Security Number is the key number data brokers use to tie consumer profile information together. Somehow, the thinking goes, without an SSN, there is no privacy violation. While credit bureaus do index people via SSN, among other pieces of data, many data brokers use a consumers' phone number as a powerful and preferred indexing and authentication tool. A consumer's phone number – beyond being sold as a piece of valuable data in its own right – can also be used to assist in disambiguating consumers with similar names, addresses, emails, and other information.

Many types of data brokers exist, and it is important to understand that the same piece of data -- a phone number -- can be used in multiple ways by differing business models. Some data brokers host their own data and are significant purchasers of original data. LSSi is an exemplar, because it purchases information from phone companies and others and compiles the information for resale, for example, on "new movers" lists.[48] Some data brokers analyze data and come up with consumer scoring and other profiling. LSSi appears to do some of this kind of work as well. Some data brokers sell or resell or share consumer information online in a public way. Targus disseminated Comcast information to anyone with a web connection via Ecolisting.com.

Another common data broker model involves the flow of information from the largest name-brand companies to the smaller companies, who then turn around and resell the data to a third tier of "affiliates" who then market the information themselves, or to another downstream affiliate. In the affiliate model of data brokering, information disseminated from a site like Ecolisting.com typically can spread far and wide, like wildfire.

(continued from previous page)
Hopping, Rick Monaco,& Sarah Rittman,What Do Your Consumer Habits Say About Your Health? Using Third-Party Data to Predict Individual Health Risk and Costs. Proceedings, SAS Global Forum 2013. <http://support.sas.com/resources/papers/proceedings13/170-2013.pdf>.

[48] *See* http://www.lssidata.com/data-services/new-mover/fc-2-0.html.

VII. COMCAST'S USE OF SUBSCRIBER LIST INFORMATION IN THIS CASE

Q13: What is your understanding of the role of Targus in this case?

A13: It is my understanding, from the OII and the few other documents I've reviewed in this case, that Targus performs a variety of functions for Comcast, one of them being as a licensing agent for Comcast's subscriber list information.

Q14: Do you have concerns about the role of Targus as an "authorized agent" of Comcast for the licensing of Comcast subscriber information?

A14: Yes I do. I understand that Comcast contends that it is required by the 1996 Telecommunications Act to provide its directory lists to other carriers, for directory publishing and directory assistance purposes. But Targus' use, display, and sharing of Comcast customers' phone numbers and related information (subscriber or directory list information also includes names and addresses) is deeply problematic. Targus is a data broker. "Targus is a commercial aggregator and provider of consumer and business data to third parties. The third parties can use the consumer and business data themselves to provide directory assistance and publish telephone directories."[49]

After Comcast gave Targus its customer phone numbers -- including non-published numbers -- Targus displayed the numbers through its vast Caller ID database, and it published the phone numbers online at Ecolisting.com where other additional data brokers could then find and reuse the information without contractual stipulations or restraints -- the data was then in the wild.

Although it is not part of what is in question in this immediate case, on Comcast's' behalf, Targus likely also used the phone numbers to create what is known as a data broker profile of its customers, noting the phone number attached to the consumers' addresses, net worth, and other characteristics. There is no question that Targus acted

[49] Lssi v Comcast - Ainge 2 declaration; *see also* www.neustar.biz (Neustar purchased the Targus business, and now advertises itself as an "information services and analytics" business.

then as a data broker and still functions as a data broker, and its Businessweek profile describes its activities as such:

> Targus Information Corporation provides real-time and on-demand information services. The company offers IAN (identifiers, attributes, network), an insight engine for marketing analytics, customer acquisition, identification and verification, scoring, location, caller id, customer retention, display marketing, and real-time analytics. The company was founded in 1993 and is based in McLean, Virginia. As of November 8, 2011, Targus Information Corporation operates as a subsidiary of NeuStar, Inc.[50]

Q15: Do you have any observations regarding Targus' use of Comcast unpublished numbers in its Caller ID Database?

A15: Yes, I do. As early as 2010, Targus was described as a company that had a near-monopoly on caller ID services, with 86 percent of all U.S. cable and independent VOIP subscribers[51] and more than 4 billion Caller Name displays per month. (Caller ID Name, or CNAM, is an industry term of art.) CNAM displays a phone number and a Caller ID Name, which is typically a 15-character string. CNAM can be used to display the calling party's name alongside the phone number.

When Neustar acquired Targus in 2011, the company described Targus as "the largest provider of Caller ID Services."[52]

[50] Businessweek Company Overview of Targus, http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=6726010.

[51] "TARGUS info, a leading data repository company, is responsible for the caller name services of 86% of all U.S. cable and independent voice-over-IP subscribers. The company announced today that its caller name services, which provide real-time consumer and business data, are in use by more than 4 billion CNAM displays per month." Sarah Reedy, ConnectedPlanetOnline, What is Targus Caller ID Database? March 29, 2010. http://connectedplanetonline.com/business_services/news/targusinfo-universal-caller-ID/.

[52] Neustar Insights, October 11, 2011. http://blog.neustar.biz/neustar-insights/why-neustar-is-acquiring-targusinfo/.

The Targus Caller ID service used the Comcast customer information acquired from billing records. Comcast gave Targus both published and non-published numbers,[53] but the Comcast "data table did not reflect subscribers' 'unlisted' status as it should have."[54] As a result, from July 1, 2010 to December 10, 2012, Comcast's customers who paid to be non-published were published in the massive Targus Caller ID database. The Targus Caller ID database likely included consumer information tied to the phone number, or CNAM.[55]

This is a terrible problem for each customer who wanted a non-published number. But it is potentially life threatening for customers who have special concerns or who are public officials.[56]

Q16: Does Comcast's online display of non-published phone numbers, with Targus' help, cause you further concern?

A16: Yes. Comcast has essentially admitted that it displayed non-published numbers on its ecolisting.com website from at least July 2010 through October 2012 (and possibly until December 2012).

Ecolisting.com is an online directory service web site. These types of websites are a form of an online phone book, but have deeper functionality because lookup is easier. The Internet Archive captured 222 screenshots of ecolisting.com from March 20, 2006 until May 18, 2014. (https://web.archive.org/web/*/http://www.ecolisting.com). Using this tool, it is possible to view what consumers and other data brokers would have seen online.

On December 27, 2010, the Comcast/Targus interface looked like the screenshot below, as captured from the Internet Archive:

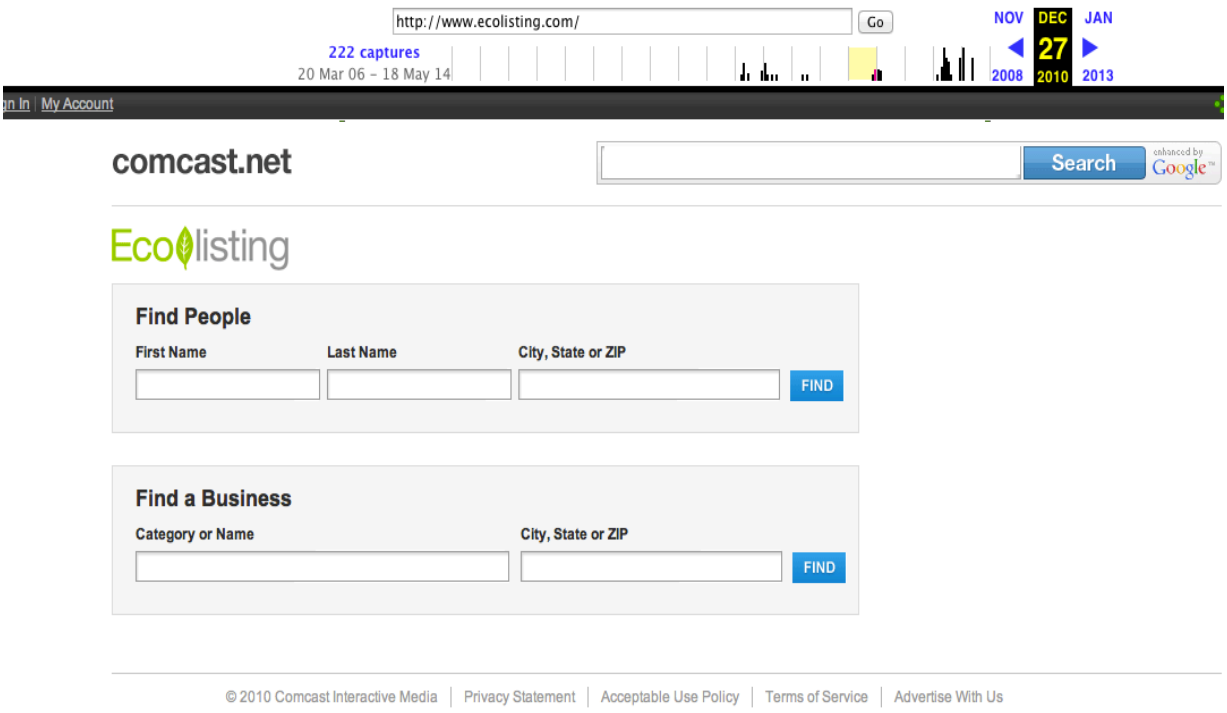
---

[53] OII, at 7 ("Comcast admits that it released to Targus/Neustar the erroneous residential subscriber list information.").

[54] OII at 3.

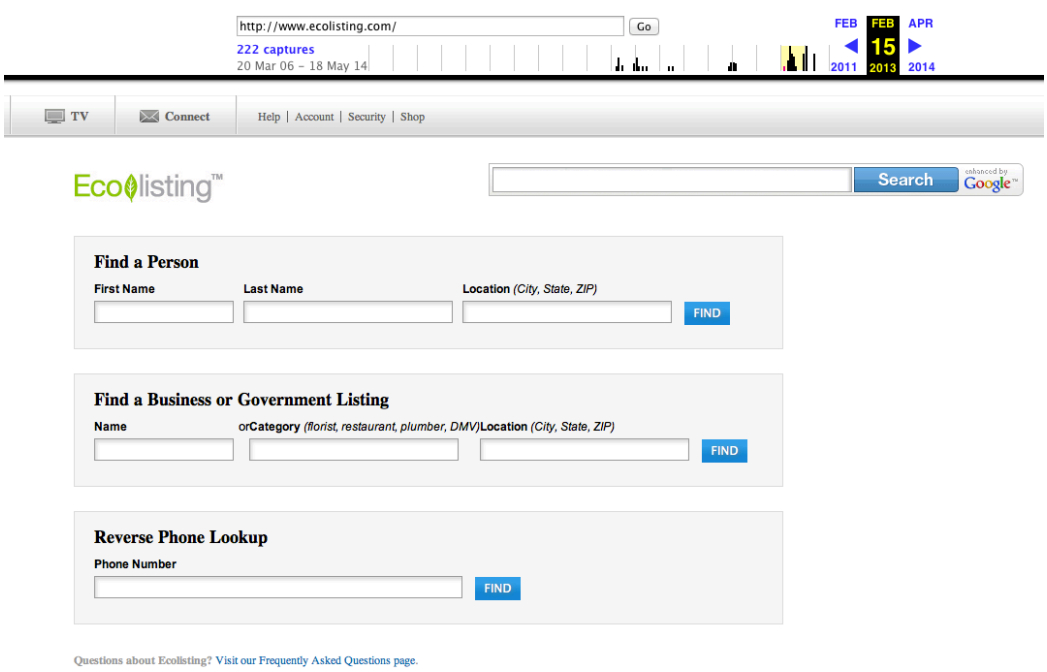
[55] *See* fn. 37.

[56] *See* Comcast customer declarations, found as Attachment X to Momoh Testimony.



This format allowed a person to look up people or businesses by name, and displayed the information of Comcast customers with non-published numbers.

At some point in 2011 or 2012, Comcast/Targus began allowing a reverse search to be conducted. All one would need is a phone number, and the customer's full name would be revealed. Although the Internet Archive did not capture a screenshot in 2012 for this, the first screenshot recorded on February 15, 2013 shows what this looked like for consumers during those years:



The Ecolistings.com reverse lookup feature is particularly problematic in that anytime a non-published customer gave out her phone number relying on Comcast to protect her privacy, anyone with a Smartphone, an iPad, or a laptop could have looked up her number and obtained her full name and address details.

Q17: Do you have concerns about Targus as a Sales Venue for Comcast Directory Information?

A17: Yes, I do. According to the declaration of Phil Miller in the *LSSi v. Comcast* litigation, "all" directory publishers that wanted the Comcast customer data could purchase it. "All Directory Publishers that want access to Comcast's Subscriber Listing Information may purchase it from Targus on the same rates, terms and conditions, including on the same rates, terms and conditions as Comcast provides to itself."[57] In the

[57] LSSi v Comcast, 3rd Declaration of Phil Miller, filed on or about April 29, 2011, *in LSSi Data Corp vs. Comcast Phone, LLC,* Case No. 1:11-cv-1246, United States District Court For The Northern District of Georgia, Atlanta Division, retrieved from PACER on or about July 12, 2014, with 2007 LSSi/Comcast contract attached; found as **Attachment K** to the Testimony of Nathan Christo.

declaration, Miller explained that Comcast data went to Targus, and then went to vendor kgb USA for 411-directory assistance services.[58]

Declarations filed by LSSi Data in that case also indicate that Comcast data went to LSSi for sale to kgb USA (as more fully discussed below). It is unknown how many other vendors purchased this data, but there are indications that Acxiom[59] and other data brokers may have purchased it from LSSi.[60] See also Confidential Testimony of Nathan Christo, containing (as Attachment E) confidential deposition testimony from Phil Miller on this question. From the record in the LSSi v. Comcast litigation, it appears that Comcast data was going to LSSi from mid-2009 through September 2012, i.e., almost the entire time that the Comcast data breach or "process error" remain undetected.

Q18: You have mentioned LSSi. Do you have concerns about **the Role of LSSi** in the Comcast Data Breach?

A18: Yes, I do. LSSi is a data broker. It sells information to data resellers, which creates a large and complex downstream data flow to third parties. LSSi also creates data cards and data marketing lists of millions of consumers using directory data, among other data. Comcast customers who had requested unpublished numbers had their information sold directly to LSSi during the breach period in question from 2010 through at least September, 2012.[61] Documents indicate that LSSi sold customer data to additional third

---

[58] *Id.* at ¶¶ 3-5 (found as **Attachment K** to the Testimony of Nathan Christo).

[59] Acziom was identified as one of the "three … largest companies" in the "data broker" category, which "operate behind a veil of secrecy." …[Senate Committee on Commerce, Science and Transportation, "A Review of the Data Broker Industry: Collection Use and Sale of Consumer Data for Marketing Purposes (December 2014), available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a. at iii.

[60] *LSSi v. Comcast,* Declaration of RICHARD OLDACH [LSSi President), filed February 25, 2013, at ¶ 14, and Exhibit F, reproduced as **Attachment CC** to the Testimony of Nathan Christo) (Acziom email wondering about continued access to Comcast subscriber information).

[61] In a publicly filed declaration in U.S. District Court, Mr. Miller states that the "LSSi Agreement was effective May 15, 2007," although he later qualified that to say that "LSSi did not begin to accept daily feeds of data from Comcast until March 24, 2009." First quote is from Declaration of Phil Miller, filed April 19, 2011, at ¶ 5 (found as **Attachment F** to Christo Testimony herein); second quote is from Second Miller Declaration, filed April 21, 2011, at ¶ 5 in the *LSSi v. Comcast* case. Although Comcast

(continued on next page)

parties without Comcast's prior approval during the time of the breach, which was in violation of their agreement. Paragraph 7.3 of the LSSi contract with Comcast states "…the Parties shall work cooperatively to address any payments for the sale or license of DA Listings Information to unaffiliated third parties."[62]

On June 17, 2011, Comcast's attorneys at Davis Wright Tremaine wrote to LSSi's attorney saying that LSSi had "breached Section 7.3 … by providing certain third-parties with access to Comcast's directory records without receiving Comcast's prior approval and by failing to share revenues derived from providing that access."[63] Comcast's counsel demanded $420,265 for this data, later upping that figure to $530,247.[64] This is a significant development because this sale of customer information put the data in play deep in the data broker chain, as discussed below.

The Comcast sale of data to LSSi overlaps with the sale of Comcast customer data to Targus. So for a period of time, these customers had their data flowing to two large data brokers.

Q19: Why is Comcast's sale of the data to LSSi problematic?

A19: That Comcast sold its subscriber data set to LSSi is highly significant. LSSi is a traditional data broker or reseller as the GAO defines it.[65] LSSi claims correctly on its web site that "Data resellers rely on LSSiDATA." (See below,) LSSi's business model is

---

(continued from previous page)
attempted to terminate the LSSi Agreement effective May 15, 2011, the District Court granted an injunction which remained in effect until September 2012, requiring Comcast to continue to provide listing information to LSSi. *LSSi Data v. Comcast Phone, LL*C, 696 F.3d 1114 (Eleventh Circuit, September 2012). (vacating District Court injunction).

[62] The contract is found attached to the first Miller Declaration, dated April 19, 2011, found as Attachment F to Christo testimony.

[63] Exhibit 3 to a July 12, 2012 declaration of that LSSi attorney, Robert Williams II, filed on July 12, 2012 in the *LSSi v. Comcast* matter, found as Attachment M to the Testimony of Nate Christo.

[64] See Exhibit 4 to Williams Declaration, a September 14, 2011 letter from Davis Wright Tremaine to LSSi (also Attachment M to the Christo Testimony.

[65] U.S. Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663, at 2 (2013)("Information resellers—sometimes called data brokers, data aggregators, or information solutions providers…").

that of selling its information over and over again to data resellers, who then also sell the information further downstream.

After Comcast gave consumer non-published information to LSSi, it would be impossible for a consumer to unravel the data flows or the loss of privacy. LSSi would have no mechanism to "recall" customer data inappropriately sold to third parties over the course of time in the past, and those to whom LSSi sold the data would similarly not have the ability to unwind the further privacy breach. It is 100 percent likely that Comcast customers who had their data sold to LSSi have had their data shared with a data broker, because LSSi *is* a data broker. And not just a data broker, but a data broker which sells to other data brokers and resellers.

In 2011, during the period of the breach, LSSi described its data brokerage activities as follows (from Feb. 2, 2011 via Internet Archive):

LSSi describes on its web site the data sets it uses for its work.

>> Data Sets

LSSiDATA offers the most extensive breadth and depth of residential, business, and government name, address, and telephone number contact information with associated detail acquired via a unique range of sources. Key LSSiDATA value points include:

- **At the source** – ***LSSiDATA compiles contact information directly from telecommunications carriers in North America.***
  - Data resellers rely on LSSiDATA for the most recently updated
  - Residential and business contact information.
  - Carriers depend on LSSiDATA as the data resource for 411 services.
- **Coverage & Volume** – Contact information obtained from wireless providers, local exchange carriers, VoIP providers, and cable companies result in extensive nationwide coverage totaling hundreds of millions of records.
- **Quality** – VoltDelta's unique QUIC process (Quality Update Identify & Change) process utilizes unique experience and technology to deliver remarkable freshness and accuracy for high volumes of data.

LSSiDATA's National Directory Assistance Database is the most current, accurate, and timely source of name, address,

> and telephone number data available. The key to its value is that the data set receives over one million updates daily.
>
> Additional data sets include New Connect Data, Wireless Data, and a file of telephone listings that are comprised of VoIP and other listings that are neither standard "land-lines" nor wireless listings, which are referred to as LandLine Plus.
>
> All of LSSiDATA's data sets go through extensive QUIC processing to enhance quality and value. From postal processing to geo coding to additional data element append, LSSiDATA enhances timeliness, accuracy, and coverage to deliver a competitive edge.
>
> As part of the Volt Information Sciences family of international organizations, LSSiDATA provides confidence as a data partner with resources to invest in innovation and to remain committed to quality standards and financial stability.[66]

LSSi sells this information for the following markets, which include credit and collections, new mover lists, data append lists, and even political campaigns:

> The ability to effectively identify, reach, or respond to individuals or businesses depends upon acquiring names, addresses and phone numbers and associated detail with exceptional accuracy, currency and completeness. **LSSiDATA** delivers these results and more for a wide range of market requirements.
>
> As the only enterprise-based data vendor sourcing telephony-based business, residential and government contact information directly from and for all of the major telecommunication providers in North America, LSSiDATA is "closest to the source". As a result:
>
> - Direct Marketers will reach **New Movers** earlier in their "hyper-buying" window
> - **Credit and Collections** will quickly locate targets with multiple data sources

[66] http://www.lssidata.com/data-sets.html (bold italics added) (site visited July 14 and 17, 2014).

- **Risk Managers** will increase confidence with additional contact detail
- **Contact Centers** will optimize care with more intelligent call handling
- **Telematics** providers will provide more current business names & locations
- **Retail** organizations will boost integrated marketing with address appends
- **Political campaigns** will target fund raising more effectively by congressional district

View how **LSSiDATA** will address the needs for your markets."[67]

From the record in the *LSSi v. Comcast* litigation, it appears that Comcast never conducted (and maybe was never able to conduct) an audit of LSSi to inquire or affirm to whom the Comcast customer data was sold, nor how frequently. Based on LSSi's data use capacities and policies, the likelihood of Comcast customer data being spread to multiple third parties, including data marketers, is extremely high.

VIII. PROBLEMS AND HARMS WITH THE PUBLIC DISSEMINATION OF NUMBERS

Q20: Given the facts recited above, do you see the Comcast non-published customers who were victims of the privacy breach exposed to potential harms, and/or do they exemplify other problems in the data broker world?

A20: I see the following problems.

A. Lack of choice for consumers

Comcast customers who paid to have their information unpublished should have been able to keep their information out of the extensive data broker exchange and sales chain to begin with, because after the data enters the chain, it is impossible to control. This is because the phone number, name, and address information is inevitably exposed to second and third parties. After these parties receive the data, it is very challenging to

[67] http://lssidata.com/markets.html (visited July 14 and 17, 2014).

track, control, or recall it. In essence, the data breach removed Comcast customers' privacy choices completely.

In its breach notice to customers in January, 2013, Comcast stated that "We recently became aware that your XFINITY Voice telephone number was inadvertently published in our online directory, Ecolisting.com, through which a third party publisher could have obtained your information, even though you previously requested a non-published or non-listed status."[68]

This notice vastly understated the problem. The Targus online public record database laid the groundwork for a huge network of data brokers to disseminate the information that was supposed to be unpublished, and provided a free source of customer data for many secondary data brokers, third party data marketers, bill collectors, and other companies.

This is no small problem. All individuals who asked for this protection were entitled to it by law. But some individuals, victims of domestic violence, crime, and members of law enforcement are particularly vulnerable to physical harm and threats, as demonstrated by the Declaration of Jane Doe 4:

> 2. Beginning in approximately 1992, and after my husband became an Administrative Law Judge with the California Unemployment Insurance Appeals Board, we paid to have our telephone number non-listed and non-published. We did so based on the strong recommendation of the Appeals Board and to protect our family's privacy and security. The importance of an unlisted and non-published number was driven home to us in 2008 when my husband received threatening letters from someone who was later determined to be a family member of a party to an appeal proceeding. He apparently found our address and private information about me and our children on the Internet.
>
> 3. By non-listed and non-published, we understood that there would be no public access to the number, not in directory assistance and not in telephone books.

[68] PUBLIC_Exh.1 (Jane Doe 11).pdf.

4. In January 2013, we received notice from Comcast that our non-published number had been published.

5. I called them to tell them that this was really not OK, given the particulars of my husband's employment, and our past experience with threatening letters. They offered me a service credit if I would agree to a release of liability. I asked them to put this in writing.[69]

B. The Data Broker Information Chain and How it Impacted Comcast Customers

When Comcast customers' phone numbers were published online as public information on the Targus Ecolisting.com web site, those phone numbers became fair game for unregulated use, and could be acquired and reused at will. In other words, those phone numbers became subject to the data broker information chain, and the probability of their further dissemination was extremely high, as evidenced by Comcast customers' experiences and by what we know of the data broker industry and how it works.

This is not a mere theoretical exercise. Unfortunately, this sequence of information exchange is the reason why publication of the unpublished numbers represents such a threat to Comcast customers. The information didn't just "go into the ether" with no effect. There is a well-oiled, well-established and complex set of business mechanisms and practices that allow for extraordinary dissemination of consumer information, especially valuable pieces of information like genuine phone numbers and addresses. Following is a further discussion of these issues.

C. Lack of Regulation

One of the causes of rapid spread of consumer information after consumer data enters the data broker chain is the lack of regulatory protection. Comcast non-published customers lost what protections they had, when their data was published on Ecolisting.com.

Consumers have no effective rights when a data broker acquires their information because no legal framework requires data brokers to offer consumers a right of deletion,

[69] Jane Doe 4 Declaration, found at Momoh Testimony, Attachment P.4.

correction, access, or any other rights. A 2013 GAO report on data resellers (data brokers) outlined in detail the lack of regulatory oversight regarding data brokers.[70] The GAO found that privacy laws apply to credit bureaus and health care providers, but data broker activity generally falls outside these laws.

In the past, detailed consumer information was largely the provenance of credit bureaus, which are subject to the Fair Credit Reporting Act. Now the emphasis has shifted from the credit reporting system to unregulated areas, including marketing and selling personal data beyond the credit report. These newly evolved data collection and use models merge online and offline data collection to form an informational picture of the modern consumer that is profoundly detailed, comprehensive, and may be used to determine a great deal about a consumer's experience and opportunities.

Non-credit, unregulated consumer reporting has been a well-established business model for many years now. Most consumers only find out about these databases accidentally, if at all. These databases contain robust and sensitive consumer information, such as financial or employment information. But this information is not used for purposes that fall under the Fair Credit Reporting Act, so the databases are completely unregulated.[71] None of this is new.

What is new and has changed within the past decade is the ease of implementing this consumer data collection model. Collecting, accessing, and manipulating these types of data stores has gotten cheaper and faster. In the past, consumer information based on non-credit, unregulated reporting was controlled to some degree by the expense of obtaining the data and the challenge of managing the databases. Technological advances have lowered such barriers, and ushered in an era of "big data."

---

[70] See generally U.S. Government Accountability Office, *Information Resellers: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace*, GAO-13-663 (2013).

[71] Id. at 16 ("In relation to data used for marketing purposes, no federal statute provides consumers the right to learn what information is held about them and who holds it. As noted earlier, FCRA … does not apply to personal information used for marketing (other than prescreened marketing offers").

Now there are more non-credit consumer databases in use, the databases are being used in new ways, and they are generally more accessible to a growing corps of potential purchasers.

D. Lack of Traceability

After the Comcast data breach, it would have been "virtually impossible" for its customers to trace where the phone numbers went due to the lack of traceability of the data in the data broker chain. The FTC, after a multi-year investigation of nine data brokers, wrote that:

> Data brokers provide data not only to end-users, but also to other data brokers. The nine data brokers studied obtain most of their data from other data brokers rather than directly from an original source. Some of those data brokers may in turn have obtained the information from other data brokers. Seven of the nine data brokers in the Commission's study provide data to each other. Accordingly, it would be virtually impossible for a consumer to determine how a data broker obtained his or her data; the consumer would have to retrace the path of data through a series of data brokers.[72]

This is a poor outcome for customers who sought the protection of an unpublished number, and it defies those customers' expectations of privacy and good treatment. Even worse, those breached customers did not and still do not have the ability to be removed from ("opted out") the databases, or to be opted out of all data use and display after the breach.

E. Inability to opt out after data transfer

Opt out is an area that is particularly problematic for consumers. After the Comcast phone numbers were published online, the many parties collecting the data did not have to offer consumers any opt outs. While Comcast removed names and numbers from Ecolisting.com, other data sites do not have to follow those same rules.

---

[72] Federal Trade Commission, "Data Brokers – a Call for Transparency and Accountability"(May 2014), available at http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf, at 4.

Opt out is not widespread in the data broker world. In testimony before Congress, the World Privacy Forum testified that it had compiled a list of more than 350 consumer-focused data broker sites and lists, which included directory sites, available at http://www.worldprivacyforum.org/2013/12/data-brokers-opt-out/. This list comprises a roughly 10 percent sample of the data broker universe, including: various people finder web sites; data brokers that the Senate Commerce Committee or the FTC has sent letters of inquiry to; consumer list brokers; and others. Of 352 data brokers studied at the time, 128 offered a data opt out. Some of those were full opt outs, some partial or unclear, some of them cost as much as $1,799.00, and one opt out promised that the site reserved the right to "publish the request" if someone decided to opt out. In short, removing a consumer's name and information from all online and offline data broker lists is an impossible task right now.

Comcast customers have already suffered the consequences of the lack of opt out. Jane Doe 11 declared that her information had spread to Radaris, a site that according to the Declaration did not immediately allow the customer an effective opt out. The customer spent hundreds of dollars to get the breached information offline, but was not entirely successful.

> Because of my safety concerns, I had to take immediate action to protect myself upon learning about Comcast's privacy breach. In January 2013, I spent several hundred dollars paying www.reputation.com to scrub my information from the Internet. This service provides me with updates when my personal information reappears online. But, it appears this service cannot completely undo what Comcast has done with my personal information – exposed it on the Internet for over two years.[73]

This suggests the limits of the monitoring Reputation.com does. They do not monitor in "real time." They only scan the Internet every 30 days. So when information reappears, it can be on the web for up to 29.9 days. It is my understanding that real time

[73] Declaration of Jane Doe 11, found as **Attachment P.11** to the Testimony of Rahmon Momoh, at ¶ 7.

monitoring costs thousands of dollars per year. It is something only celebrities and public figures can afford. A person of ordinary means is out of luck when something like this is done to her. As Jane Doe 11 stated:

> Reputation.com was also having a difficult time getting my information removed from another Internet people finder directory, Radaris.com. Reputation.com informed me in a February 24, 2014 email that they were "deeply concerned with Radaris's compliance record." They also stated that
>
> > Unfortunately, at this time, the majority of removal requests to Radaris are failing. Some of our customers are reporting that they remain visible. Again, we have contacted Radaris to improve this situation.
> >
> > In the meantime, you can contact them directly by phone or email: htpp://radaris.com/contact
>
> I am attaching this email here as Exhibit 2.[74]

When Comcast customers were offered a choice to have an unpublished number, the importance of honoring that original request was significant. Only a small percent of known data brokers offer a full, voluntary opt out after the data gets in their databases. Within that fraction, the process of opting out can be incomplete, extremely difficult, and must typically be done one-by-one, site-by-site. Often, third parties are not allowed to opt individual consumers out of data brokers.

When consumer phone numbers are published and scooped up by offshore data brokers, or by thoroughly unregulated sole proprietors, there is very little ability for consumers to effectuate an opt out if one is not proactively offered to them.

Q21: Does this conclude your testimony?

A21: Yes, at the current time.

[74] *Id.* at ¶ 8.