ATTACHMENT C

SWORN DECLARATION OF PATRICIA MATHIS, CHAIR XCASTLABS (JULY 2023)

Beth A. Oliak (SBN 230236)
Edward A. Pennington *pro hac vice* to be file)
PENNINGTON OLIAK, PLLC
1055 Thomas Jefferson Street, NW Ste. L35
Washington, DC 20007
Tel: (202) 897-2725
Fax: (202) 838-824
oliakb@pennoliak.com
epennington@pennoliak.com
Attorneys for Defendant
XCAST LABS, INC.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA, WESTERN DIVISION

UNITED STATES OF AMERICA

Plaintiff,

v.

XCAST LABS, INC.

Defendants.

Case No.23-cv-03646-ODW(JCx)

DECLARATION OF PATRICIA MATHIS

1. My name is Patricia Mathis. I am Co-Founder and Chair ofXCastLabs, Inc.

2. XCAST is a Los Angeles California-based provider of advanced Unified Communications as a Service (UCaaS) solutions to small and mid-size businesses ("SMB"). XCAST is not and has never been a telemarketing company or a company that creates robocalls.

3. XCAST has not and does not provide telecom services to any call centers or telemarketers who were known to me and others at XCASTS to have demonstrated unlawful activities.

4. XCAST serves SMB customers in diverse verticals including restaurants, healthcare groups, professional firms, schools, municipalities, underserved rural areas, police and fire departments, religious and charitable organizations-and agencies of state and federal government. XCAST'S services are sold and supported by a small two-member internal sales group to channel partners (agents and resellers) who "white label" the solution under their own logo.

5. There is no industry standard definition of "robocall" other than that it begins with a pre-recorded message. Most robocalls by that definition are legal and often necessary and life-saving (such as when hurricane warnings are issued by local governments).

6. There is no industry standard definition of an "illegal robocall" except that in the telecommunications field, the term "illegal robocall" would imply some form of a violation of a rule or regulation of the Federal Communications Commission ("FCC"), the agency that regulates intermediate common carriers like XCAST. XCAST is not now and has not in the past violated any FCC regulations, whether related to "illegal robocalls" or not.

6. It is well known throughout the telecommunications industry that both the FCC and the FTC receive numerous complaints about robocalls. These complaints are relayed to the elected officials representing their aggrieved constituents, and these elected officials bring pressure to bear on the FCC and the FTC to rid their constituents of the calls.

7. The FTC, in tum, makes every attempt to demonstrate that it is solving the problem of robocalling. The FTC takes on a public relations campaign to demonstrate that the FTC is trying to fix the problem. Unfortunately, the FTC has

published untrue statements about XCAST and others, causing in some cases death threats and loss business. Immediately after the filing of suit against XCAST, the FTC published a press release stating they had sued a VOIP Service Provider (XCAST) that 'assisted and facilitated telemarketers in sending hundreds of millions of illegal robocalls to consumers nationwide." This headline, clearly meant to show that the FTC was actively helping consumers, could not have been further from the truth. Without regard for truth, the FTC caused XCAST significant ham from the loss of customers. The Press Release can be found on the FTC website along with others announcing aggressive actions, some likely to be legitimately aimed at bad actors, others, like the one about XCAST, are damaging to the point of being destructive.

8. As explained more fully below, the allegations made by the FTC in its complalint are demonstrably false.

9. Congress empowered the FCC with tools to seek out and mitigate the number of illegal robocalls when it enacted the TRACED ACT, signed into law at the end of 2019. The TRACED ACT established the STIR/SHAKEN regime for producing trace back evidence of who might have been the sender of an illegal call. XCAST has been compliant with STIR/SHAKEN rules, regulations and reporting procedures since its inception.

10. A request for a "trace back" made to a telecom company means that there is a suspicion that a call or message may be illegal. It is not a finding that such a call or message is illegal.

11. Although XCAST has only twenty-one (21) employees and had no obligation to comply with certain TRACED ACT requirements prior to December, 2023, it became STIR/SHAKEN compliant by June, 2021 as if it were a larger telecommunications carrier. XCastLabs has always embraced "Best Industry Practices."

XCastLabs historical relationship with the Industry Traceback Group (ITG)

12. The TRACED ACT created what became known as the Industry Traceback Group ("ITG") which was to consist oftelecom industry members. Long before the ITG's call tracing became legitimized by Congress with the passage of the TRACED ACT, a private group of carriers and communications providers began a call tracing consortia to identify possible fraud on their platforms.

13. Small voice providers were unaware of this activity despite the fact that the voice provider community would have been informed commentators about how the internet actually worked. Some small providers began to learn about this call tracing through the "grapevine" or from the press. Finally in November 2018 a posting on the FCC website *encouraged* small providers to cooperate with this traceback effort.

14. Several XCAST managers heard rumors and unofficial information about the traceback project through personal relationships and two emails from info@ustelcom.com requesting confidential call records. In October 2018, the FCC conducted a survey of voice providers inviting them to describe their network procedures. XCAST complied, provided its official policies and procedures and offered to meet with FCC staff to provide additional details on its proprietary tools for call screening.

15. In November 2018, the FCC posted on its website an "encouragement" of providers to support the ITG. In December, 2018, I scheduled a meeting to meet with Jonathan Spalter,President of US Telecom-the Washington-based lobbying organization that was rumored to be the driving force behind the traceback project. Even though his staff was well-aware that I had made a several hour flight in a snow storm to meet with him, I was notified as I was arriving at the Washington airport that "...Mr. Spalter is just too busy to meet."

16. I immediately initiated a call to the office of Congressman Michael Doyle,

who was then ranking member of the House Committee with oversight over FCC with the goal of learning about the traceback program. A staff member met with me around 5 o'clock in the House Office Building and during a rushed meeting I asked for some explanation about this program and explained XCAST had yet to have a meaningful discussion with either the US Telecom group or the FCC about this program. Congressman Doyle's aide told me he "knew some of the people I had mentioned trying to contact" and would "reach out to someone to contact me. "

17. My initial conversation with US Telecom's lead lobbyist occurred in January, 2019. Another XCAST executive joined me in a pleasant two-hour conversation. I pressed him to reveal the legal authority under which the call tracing was occurring, what role XCAST would be expected to play and how participating in the program would inform our own efforts to police XCAST'S network efforts to identify and stop illegal robocalling. I raised several concerns about certain legal barriers and vulnerabilities any company might face in participating in a clearly non-statutory program. Specifically, I expressed concerns about:

(l)The lack of any official sanction of US Telecom's invocation of Section 222 of the Communications Act of 1934 as its authority to "protect our networks·," [1]

(2) US constitutional and State of California's privacy protections; [2]

---

[1] XCAST raised the issue of whether the 1934 Act was applicable in this environment since "protect our networks" in 1934 would mean Bell Operating Companies would be having this conversation among themselves since they were all part of the same anti-competitive family.

[22]FCC's Section 222c restricts telecommunications carriers from sharing customer proprietuy infonnation without customer approval except in certain exceptions specified in law. Also, the *FTC's* role in protecting consumer privacy is explicit and clear in its determination that " .....(because) common carriers subject to the Communications Act are except from the FTC's Section 5 authority, the responsibility falls to the Commission (FCC) to oversee their private practices consistent with the Communications Act. See Section 24 of 47 CFR. Further the Rule expressly applies to telecommunications carriers and inter-connected VoIP Providers: "....interconnected VoIP services which have been so defined since 2007 [will] continue to consider entities providing inter-connected VoIP to be telecommunications carriers for purposes of this Rule." (See Sec. 40 of 47 CRF

(3) The well-established FCC and FTC statutory obligations to protect private consumer information;

(4) The obligation of telecommunications carriers to abide by FCC's Rule 6 to reveal to consumers what information is being collected about them__for what J?urpose this information is being used; the right to aisapprove of the sharing of that information;[3]

(5) Potential violations of the Storage Communications Act which restricted construction of meta-data of personal information;[4]

(6) PISA related tracing restrictions that require warrants;

(7) Explicit violations of the USA Freedom Act which was passed in 2015 to address the sunsetting of the Patriot Act and to address alleged abuses by the National Security Agency in collecting private call records[5]

(8) The obligation of telecommunications carriers to abide by FCC's Rule 6 to reveal to consumers what information is being collected about them; for what purpose this information is being used; the right to disapprove of the sharing of that information;

(9) The decades long controversy over telephone surveillance that has surrounded the passage of the Patriot Act and US Freedom Act and the known reprimands from the Privacy and Civil Liberty Oversight Board's regarding the abuse of NSA's authority by circumventing requirements for PISA warrants. (Excerpts from the February 2020 De-Classified Report from the Oversight Board include:

> (U) The USA Freedom Act amended the Foreign Intelligence Surveillance Act ("FISA") to expressly bar the government from using its business records collection authority for bulk collection. This J?rohibit10n effectively ended the bulkTelephony metadata program that the government had operated under the then-existing version of Section

---

[3] Protected data elements are described in Sec. 55-84. Protected data elements include (but are not limited to) call detail records, (including caller and recipient phone numbers and the frequency duration and timing of calls.

[4] US Telecom's representative said "we" thought about this but decided it didn't apply since the SCA meant the *government* could not collect bulk records. But that it was okay for private industzy to collect meta bulk data and provide it to the government that could then use it for what pmposes it deemed appropriate. The ITG is now a government agent by virtue of its appointment as the industry consortia.

[5] Certain revelations by Edward Snowden in 2013 revealed that NSA had been providing data to nearly two dozen US government agencies with search engines built to examine more then 850 billion records about phone calls, emails, cell phone locations. This search process (called I Reach) had been gathering records not only of foreigners (the intended target of the authorized Patriot Act smveillance) but innocent American citizens who were never accused or suspected of any wrong doing. The reach system was capable of handling up to five billion new records every day. The data collected through the Breach search system was in addition to the millions of ordinary Americans' phone records surveilled under Section 215 of the Patriot Act.

215 of the USA Patriot Act. (Q) At the same time, the USA Freedom Act allows the government to obtain CDRs on a broader basis than **other business** records authorized for collection under the Act. Put simply, it authorizes the government to collect CDRs within two hops-e.g:, a person's contacts, and those contacts' contacts-of a specific se1ect10n term.

(9) the legal vulnerability of any carrier who cooperated in this endeavor for any of the transgressive risks arising from these non-statutory activities.[6]

18. In response to each of these concerns, the US Telecom's Representative responded "we" have thought about that. I made multiple inquiries about the identity of "we" and finally was told" "...people you would recognize like AT&T, Verizon and Microsoft." I asked US Telecom's representative to explain why, in light of so many legal ambiguities and concerns, they would create such a program. He replied, "We had to do it to avoid regulation. Ifwe don't do it the government will."

19. Shortly after my January 2019 meeting with the US Telecom representative, XCAST made the decision to officially join the traceback effort. In a meeting with company managers who would be stakeholders in this process, we discussed the operational and legal implications of voluntarily joining the project.

20. Despite the many concerns I had expressed to the US Telecom representative we made the decision to cooperate based on FCC's *encouragement* that voice providers participate in the progr . I appointed an official representative, the Senior Vice President for Operations, as the company's contact and XCAST began voluntarily providing comprehensive records to the traceback group in January 2018, including historical records that could assist the ITG is creating a meaningful database.

---

[6] The ITG has implicitly recognized its potential risk for sharing CDRs before the authorities granted by FCC's Rules associated with TRACED ACT implementation. US Telecom's lobbyists actively encouraged the passage of Senate Bill 3335 which seeks to protect companies from liability for sharing call records-which inherently presumes the illegality of such practices

21. When providers received an email from the ITG identifying a phone number about which they were inquiring, XCAST'S representative searched through records to identify whether the number belonged to XCAST. If a number belonged to a direct customer, XCAST'S manager contacted that entity to tell them XCAST had received a traceback suggesting something "suspicious" and requested that they investigate and provide details of any investigation. In the case of a Reseller or a Master Agent whose customer was not directly known to XCAST, they were asked to conduct a similar investigation. Once the results of the investigation were known to XCAST, these details were immediately conveyed to the ITG.

22. Significantly, participating providers like XCAST were not provided feedback or advised what to do or what changes were expected of them once a trace back was initiated.

23. Participating providers were told by ITG staff that they were constructing a database including a website (portal) with data capture functionality that could record and track certain called numbers the ITG determined to be "suspicious." The ITG made its own determination about what constituted "suspicious" and worthy of a traceback and does not inform its members or participating providers the basis for their determination.

24. Upon information obtained later and current belief, a member of US Telecom's Executive Committee engaged a project manager to build the aforementioned database. This project manager had access to all data elements and call tracing information provided by the participating providers. This information was not available to the providers, even the ITG's Steering Committee. This project manager was ultimately released from his role in the tracing project due to alleged improprieties. Informed sources revealed that the party had begun calling up legitimate business Call Centers and calling them "criminals." Some of the Call Centers began contacting the FCC to protest and this activity led to the ITG's

decision to end their relationship with the project manager.[7]

25. Participating providers eventually were able to access the portal developed by the ITG that allowed providers to see their own data. This information was therefore limited in identifying the source of suspicious calls because it initially only replicated the information the provider had given the ITG. Eventually participating providers were able to see only the immediate upstream and downstream providers-but that visibility did not occur until late in 2022. This meant an intermediate provider like XCAST continued to be blind to the source of a call initiated by someone else. Without illegally accessing the message itself, XCAST could not know whether a call was illegal or not.

26. In the meanwhile, all voice providers were obligated under the terms of the STIR/SHAKEN rules to pass the call with the same attestation it received. These statutory limitations *limit* any provider's discretionary decision about traffic crossing their network because they are *obligated* by TRACED ACT Rules to authenticate the traffic according to the rules established by the FCC.

27. Participating providers have made numerous pleas to obtain the identity of the "bad actors" from the ITG. The ITG staff say this cannot be revealed because "...it would violate the Sherman or Clayton Act's anti-competitive clauses." Participating members have also been further cautioned against "talking among themselves" because that might also be considered to be anti-competitive.

28. The ITG has consistently warned regulators to avoid depending on raw data because it can be misleading. It does not appear that the FTC has ignored this caution. The ITG has sent numerous formal letters to the FCC and in its annual reports to Congress cautioning against relying in raw data. For example, in a

---

[7] This !X'.rson has since become a Defendant in a law suit alleging, among other things, that he later benefited financially by relying on data he accessed as part of his engagement with the ITG.

September 1, 2022 letter to Marlene Dortch, Secretary (FCC), the ITG wrote:

- "...tracebacks results can be misleading without appropriate context."
- "...tracebacks can incorrectly state the responsibility of a voice provider, including lesser known smaller providers."

29. In the Complaint, XCAST is identified as a "point of entry" or POE (also sometimes referred to as an origination point where a call originates) as an example of an illegal robocall. However, in interpretating the ITG's traceback history, the FTC reporting ofXCAST'S identity as a POE does not comport with data XCAST can review within its own portal. The FTC has assigned dates in its Complaint that do not comport with dates in the ITG portal. This indicates at worst a false claim and at best an issue that needs to be investigated further by the FTC. Such an investigation would have been welcomed by XCAST.

30. Part of the problem is that the ITC built a database which allows companies like XCAST to enter a portal and review its own call records but not those of others. If there is a bad actor in the system, it might be known to the ITC, but it is well known in the industry that the ITG will not share caller information with carriers like XCAST, but they do share that information with the U.S. government, likely with the FCC and possibly the FTC and maybe others including intelligence agencies.

31. These "disconnects" at the FTC, where XCAST is falsely accused of being a POE for a call that may or may not be illegal, has made it virtually impossible for XCAST to evaluate all of the FTC's Claims. In any case, XCast is not an Aggregator and has never been an Aggregator and therefore has never had direct and actual information about who a caller might be.

32. Significantly, the FTC'S Complaint fails to note what *corrective action* XCAST actually took to remedy the problem or perceived problem cited in any of the tracebacks cited in the complaint. These data are retrievable with the ITG portal

under the "comment" section which FTC has apparently ignored. However, in the earliest days ofXCast'S cooperation with the ITG-which is the period the FTC is most preoccupied with in its Complaint-the portal was still being built and exchanges about remedial steps were usually memorialized by telephone, texts or email exchanges.

33. A review of these exchanges will reveal that XCast was not only a fully cooperating provider but usually within an hour launched an internal investigation in accord with its long-standing policies and procedures; it would have immediately reported its findings back to the ITG.

34. The ITG portal reflects these reports or should report XCAST'S remediation and total cooperation with concluding the traceback. The FTC also fails to properly note that the portal usually identifies a wireless provider as the terminating provider. This is significant because 85% of all calls to US numbers are terminated by wireless providers.

35. Wireless provides have legal obligations to provide Caller ID information to their subscribers and in most cases they provide accompanying features that allow the called party to manage their calls with contact directory features. This means that when an incoming call reaches a subscriber, that person can make the individual choice about whether or not to answer the call. And, if the call or message appears to be a scam, the called party can report the actual message to the FTC who can then take definitive actions against the scammer, and not attempt to shut down the telecommunications network to block calls that may be scams.

36. The FTC's Complaint is founded on flawed logic: two examples of *reducio absurdum* fallacies. First, at Paragraph 24, the FTC embraces an ITG theory that a "suspicious" phone call is one that traverses one or more voice provider networks. If that were true then virtually all phone calls made around the world and in America would be illegal. Most telephone calls are originated from the calling party through

a broadband provider (the on-ramp to the internet) onto the interconnectable global highway, before finally exiting the Public Switch Telephone Network (PSTN), meaning your home phone or cell phone, before being delivered to the called party by either an ILEC or (in 85% of the time in the US) to a mobile provider. Secondly, the Complaint incorrectly claims that "suspicious" equals "abusive, unlawful or fraudulent." There is not a single suspicious call identified in the complaint that was found to be illegal or "abusive, unlawful or fraudulent." To make that determination you would have to identify the message, and no messages have ever been identified to XCAST.

37. The entirety of the Complaint deals with suspicious calls, and even those were very few and never found to be actually fraudulent. Had the FTC conducted a proper investigation of XCAST'S business, the truth would have been discovered, and false claims would not have been filed against XCAST.

38. To compound the unjustified assault on XCST, the FTC bundled these false and unproveable premises into a syllogism that results in an absurd conclusion. The FTC takes the position that if a call is suspicious, it is illegal. That is simply not true, nor has it been shown in the Complaint to be true. To compound the problem, the FTC is apparently using an undefined and constantly shifting definition of "suspiciousness" in a way that makes compliance with FTC demands a function of who they wish to pursue.

39. The Complaint at Paragraph 25 misrepresents the facts of what was sent to XCAST. The FTC asserts that in January of 2020 a "warning letter" was sent to XCAST, telling them they will get in a lot of trouble if they engage in support of fraud against consumers. However, this letter was sent to many carriers, and in the case ofXCAST, the letter did not provide XCAST with any information about any specific alleged wrongdoing. XCAST was not told to stop doing anything.

40. In the Complaint at Paragraph 26, the FTC appears to believe that because

the ITG has provided certain information it has collected about calls that have (a) already been completed; and (b) a called party has complained about the call to the FTC, that a voice provider could necessarily have done anything about it- especially during the period 2018-2021 (which is the time period that the FTC has complained about). XCAST provides business-to-business services and does not know who a calling party is. XCAST has no way of knowing the content of a call- unless the called party describes the content after the fact. There is no allegation in the Complaint that anyone identified the content of a call or message to XCAST.

41. The landscape for how internet-based calling would occur was significantly changed by the passage of the Traced Act, which was signed into law on December 30, 2019. The FCC's subsequent rules outline a detailed call attestation process that causes each provider to "sign" a call passing through it network in a specific way and with an attestation (or authentication) that is regulated by the FCC. Neither the ITG or the FTC play any role in that regulated process. And XCAST is in full compliance with these requirements.

42. Paragraph 27 of the Complaint incorrectly identified XCAST as the Point-of-Entry (PoE) regarding an automated message about the SSA threatening a lawsuit, The ITG sent a message to participating providers: "Originators please search for records for similar traffic and take prompt mitigating steps to stop all such calls." The ITG's portal did not identify XCAST as the PoE as the FTC claims.

43. Instead, XCAST was identified as Hop 3 and the PoE was identified as an Australian company. XCAST immediately assisted the ITG in researching the identity of the Australian party and asked the Agent with the relationship with the company to investigate and terminate any party whose traffic might be inappropriate. XCAST also terminated the relationship with the Agent's customer when they were unable correct the problem. Had the FTC done an adequate investigation of XCAST, they would have found these facts out.

44. The Complaint alleges that XCAST failed to take (unspecified) actions against parties associated with subpoenas requesting information about phone numbers. However, the FTC staff (a) Does not seem to know that carriers and providers who receive such subpoenas are not told the reason for a subpoena; and (b) Did not bother to read XCast's responses to the subpoenas. Had they done so they would have known the number about which the subpoena inquired does not belong to XCAST.

45. The Complaint at paragraph 37 accuses XCAST of misconduct by implying XCAST was associated with some party named E. Sampart mentioned in a subpoena from Georgia. The subpoena asked XCAST if a certain identified DID has been assigned to Sampart. XCAST responded that XCAST had no record of such a number or an affiliation with the named party.

46. This alone represents the extent to which XCAST'S phone numbers could have been spoofed by criminals. An adequate investigation by the FTC would have revealed this.

47. In various paragraphs of the Complaint, the FTC mentioned two entities: DialCom and RSCom. These parties came to XCAST'S attention in a January 2021 Civil Investigative Demand (CID) the FTC sent to XCast asking for call records associated with these companies and recordings of all phone conversations XCAST employees had with them. The FTC's staff working on the CID did not believe XCAST when XCAST advised that it had no such recordings. In fact, XCAST'S Personnel Manual strictly prohibits such recordings. The same CID demanded other records XCAST never possesses because it was never engaged in any business activity that would have required such records. These requests indicate that the FTC thought that XCAST was a robocaller or telemarketing company. An investigation by the FTC would have revealed the true nature of XCAST.

48. The January 2021 CID specifically asked for these details concerning an

entity known as DialCom (an Aggregator associated with a Master Agent who occasionally made referrals to XCAST). XCAST terminated its relationship with DialCom the previous year for business reasons. The same CID requested what information XCAST had about a Canadian based telecommunications services provider. An adequate investigation would have revealed these facts.

49. In its current complaint the FTC has chastised XCAST for "transmitting nearly 143 million calls for Dialcom between 2015 and 2018 and that 62 million were on the DNC Registry. XCAST has no way of knowing whether they were on the Registry for the reasons described many times. XCAST can establish contracts requiring all its partners to abide by all appropriate laws but carriers are not obligated or encouraged by the FCC to install this registry for reasons already described. In any event, XCAST ceased doing business with Dialcom as stated above.

50. XCast has no way of ascertaining or policing whether or not a partner has installed DNC - type call screening because only the signatory has access to its own SAN database managed by the FTC.

51. In Paragraph 39 of the Complaint, the FTC says that DialCom received three tracebacks that had traversed XCAST'S network and this "...provided incontrovertible proof ofDialCom's wrong-going." In an abundance of caution, XCAST then terminated it relationships with DialCom. However, as it turned out, there was no incontrovertible proof that DialCom has ever done anything wrong. Upon investigation and verification as recently as this past week (September 2023) Dialcom has never been accused by any federal agency or the ITG of doing anything wrong; on information and belief, DialCom has never officially been investigated and found to have done anything to violate any rules or regulations or orders of the FTC or FCC.

52. In Paragraph 41, the FTC alleges "XCAST'S interaction with RSCom provide

an even more troubling picture than Dialcom." The Complaint goes on to allege that XCAST has had a relationship with RSCom since April 2016 and had transmitted 370 million calls for them and 125 million were on the DNC Registry. The FTC insists XCAST must have known these calls were illegal, yet the FTC provides no "incontrovertible proof' that any of these calls were illegal. Most importantly, RSCom has recently confirmed to me that they have never been charged or investigated for any wrong-doing by any federal agency.

53. At Paragraph 39 of the Complaint, the FTC simply has their facts wrong. Regarding a September 24-25, 2020 traceback, the ITG did *not* identify the Aggregator as the Upstream provider but then its portal later identified the Aggregator as the originator or POE. The Upstream data field was left blank in the ITG portal-so it made it appear as if XCAST was the originator. This is false. In earlier tracebacks, the Aggregator was identified as the originator. The named Aggregator was the actual party "suspected" of sending "suspected illegal traffic" from his customer's customer. Traceback call records indicate that New Cingular Wireless terminated the suspected "auto warranty" calls. The traceback source details indicate that Dialcom was the call source and that *all calls were Op/in*. There was another traceback on September 15th about electricity being turned off that terminated to a Birmingham Alabama location by Bell South. None of these calls implicated XCAST, and a simple investigation would have revealed the true facts.

54. Given the number of mistakes made by the FTC, it is clear that the main problem is not illegal robocalling, but that the FTC does not know how the telecom network works, particularly one as complicated as an international packetized data network which involves multiple telecom entities as "hops" between a calling party and a called party. The FCC, whose area of expertise is the telecom network, has made no rulings or complaints against XCAST.

55. The Complaint at Paragraph 45 also contains errors of fact which could have been found out prior to filing suit with a simple investigation. This paragraph deals with a January 20, 2020 traceback (1394). XCAST'S research does not align with the allegations of Paragraphs 45 and 47 and are easily debunked. The following information reflects our best estimate for FTC's reference. Message from ITG:

> *"Automated voice offers zero interest and says press 1 to connect to life rep. Caller ID is neighborhood spoofed so ANI blocking is not an effective mitigation approach. Latest calls placed after provider in Pakistan indicated caller was no long spoofing but that is not the case. This call is just one example of millions of similar calls.. Originators please search your records for similar traffic and address with your customer.* Calling number was 800.xxx.xxxx) Toll free call. Called number was **954.xxx.xxxx.** *Terminating carrier was PCS wireless who terminated to Florida location. On January 22, 2020, (Voice Provider) notified that XCast had been carrier. XCast records indicate they were unable to find the record and believe XCast was incorrectly identified by (Voice Provider.)*

In other words, the ITG records reveal that XCAST was incorrectly identified. The FTC failed to undertake the most basic research into this issue, and could have addressed this in a proper investigation.

56. Paragraph 47 also reveals a false claim against XCAST in reference to a December 4, 2020 traceback (3795).

No exact matter between ITG record and FTC Claim. Three potential matches. "Recorded message says your electric service will be disconnected in 30-45 minutes. Utility company is not always identified. Assorted toll-free or other numbers used as called ID. Calling number is 346.326.1674. Call terminated by

Aerial Communication (wireless) to Texas.

The ITG portal does not reveal any response from XCast so we do not know its Hop location. But the ITG portal does indicate that (Voice Provider) traced a call back to XCast re complaint #3776 re SSA fraud and XCast blocked the number. Portal says that "provider is non-responsive" but does not identify the provider. Call was terminated by Verizon.

Once again, the portal information reveals that XCAST did all it could, including that XCAST blocked the call. The portal indicates that XCAST reacted properly to the traceback.

57. The Complaint identifies another traceback at Paragraph 49, where XCAST did all it could. This is a standard traceback in which XCAST would have been only an intermediate carrier. XCAST is identified as Hop 3, meaning that there were many other carriers involved, all likely having the same lack of specific information about a specific call. XCAST received the call from (Voice Provider) as Hop 4 then sent the call to Hop 2 (Voice Provider) Call was terminated by Omnipoint Communications in New York. This traceback reveals nothing more than XCAST was a hop in a call.

58. Paragraph 54 identifies a traceback (4389) from February 24, 2021. This appareas in fact to be six tracebacks that could fit the criteria for Paragraph 54 of the Complaint. All of them list XCAST as the origination but that is false. However, in all the call source comments "(Voice Provider) is the one listed as the source. The originating number was 202.845.7149. The call was terminated by Cingular Wireless. On February 22, 2021 number 865.xxx.xxxx was terminated in Knoxville Tennessee by Cingular. This was the traceback message: *Fraud Calls offering to file a suspension extension of the called party's behalf after "the federal government suspended student loan payments until the end of the year." Automated calls to wireless numbers generally not permitted. Voice-mail message does not identify the*

calling entity,, nor does it provide an opt-out option.

ITG traceback portal provides this information:

Call source details: (Voice Provider), contact information is 952.xxx.xxxx. Portal reports steps taken: Customer terminated end user causing these calls on 2/4/ at 20:26 pm. End user also implemented speech recognition on platform to reduce any further complaints. Xcast discussed matter with (ITG staff) due to the number of complaints within a short period of time.

Thus, the records show that XCAST was involved in the traceback, and nothing indicates that XCAST did not respond or did nothing to correct a problem of its own creation.

59. Paragraph 59 of the Complaint also makes false allegations against XCAST.

The FTC asserts an infraction on January 12, 2021._There were multiple tracebacks during this period. It appears to be only one where XCAST was notified on the 12th about a fraud involved the word Marriot. Trace number 4021. (There appear to have been three tracebacks about Marriot in January-numbers 4006 and 3970-but they were prior to January 8th. Two other tracebacks took place on the 12th but they do not include the word Marriot. There were traceback numbers 4050 and 4061. In the traceback in XCAST's possession, it says:

"Recorded voice offering incentive using Mariott name without permission.

Some calls placed to mobile phones. Some calls using random or unauthorized Caller-IDs. Failure to identify the entity responsible for the call. Some calls fail to offer opt-out and/or omit call back number. "" XCast was intermediate Hop 4; received the call from (Voice Provider); passed the call to (Voice Provider) Call was terminated by Verizon in Virginia

Here, XCAST was simply a "hop" and was not called upon to take any action. The traceback record is clear that XCAST was simply identified as an intermediate hop.

60. Allegations against XCAST at Paragraph 56 are likewise unfounded. This was a standard traceback; no documentation for reason or evidence as to what if anything XCAST is alleged to have done. XCAST did not originate this traffic. It was Hop 7. The call was terminated by Verizon. The FTC Complaint keeps confusing dates for when the event supposedly happened and the data the traceback was sent to XCast. But XCast was not the originator; it was Hop 6; received call from Hop7 (Voice Provider) and then sent the call to (Voice Provider); Call was terminated by Verizon in Tennessee.

61. In general, all the alleged tracebacks are inconclusive as to anything that XCAST did wrong, and more often probative of what XCAST did right. The FTC's complaint makes numerous references to the ITG's data. However, the FTC chose to completely *ign,ore* the ITG's caution against relying on raw data.

62. XCAST has no way of knowing whether calls were actually terminated, were sequential or non-sequential, whether they were lawfully obtained from the North American Numbering Council or one of its certification agencies, whether they originated from different IP addresses or whether they were phished, spoofed or mechanically autodialed in some mischievous way or the result of some silent penetration into our network. Based on information and belief we do know certain things to be true:

- The FCC does <u>not</u> consider all robo-calls to be illegal. In fact their website says just the opposite. FCC has not required voice providers to install DNC Registry and is not likely to do so. An "unwanted call" is not an illegal call. A number on the DNC Registry cannot be determined to be illegal or just an "unwanted" call. A person might put an ex-spouse's phone number on the DNC Registry but that does not mean that number is illegal or that a provider ought to be blocking all originating number directed to the ex-spouses annoyance.

- A voice provider (like XCastLabs) can prescribe contractual obligations to its customers-including call centers-to abide by a all FTC rules, but it has to ability to enforce that obligation. For instances, the FTC does not provide a public data base to reveal who has subscribed to the DNC Registry by reporting a Subscription Account

Number (which is the database that records who has actually received a SANS number to authenticate they have paid for such registration.

- Call duration is not a recognized call blocking metric according to the FCC guidelines that telecommunication service providers are obligated to follow. Nor is the FCC likely to prescribe acceptable call lengths for numerous reasons. In the case of XCastLabs alone, the company has illustrative end-users within its customer base who routinely make short duration auto-dialed calls. Examples include:

  - One of the world's largest package transporters send short pre-recorded messages: "This is a message from XYZ. Your package will be delayed for 24 hours." The company cannot listen to the call, we have no way of knowing whether XYZ properly identified itself."

  - One of the country's largest ISPs routinely sends short messages: "Your technician will arrive in one hour. To confirm, hit 1; to confirm hit 2."

  - "If you would like to hear a message from Congressman X, press 1." A called party might not want to get a message from that Congressional representative but the call is perfectly legal. XCast's platform support millions of such calls.

  - "If you would like to hear today's meditation, press 1." A called party might not want to get called by this party and puts the number on the DNC list, but it is perfectly legal. XCast's platform supports billions of calls from one of the world's largest religious communities.

  - One of the company's Resellers had the federal government as a client-including the Social Security Administration-so a call passing through the company network from an SSA number is not necessarily fraud.

- The FCC determines the conditions under which any call should be blocked and these rules were spelled out after months of public comments associated with the FCC's rule-making authority. After the passage of the TRACED Act, the FCC prescribed an elaborate system of attestation for acceptance or rejection of call traffic as it moves from network to network. XCast has always abided by those rules as required by STIR/SHAKEN implementation [8]

[8] /Under Sections 5 and 6 of the *FTC* Act (15 USC§§ 45 and 46), the *FTC*'s enforcement and investigatory authority over "unfair or deceptive acts or practices" exempts "common carriers subject to" the Interstate Commerce Act {ICA) and the Communications Act of 1934. 15 USC§§ 44, 45(a)(2), and 46(a). "Congress did not intend the *FTC* to regulate common-carrier business practices, ... because the Interstate Commerce Act had already delegated that role to the FCC. Hence, Congress established Section 5's common-carrier exemption to avoid interagency conflict." *FTC* v. AT&T Mobility LLC, 883 F.3d 848, 854-855 (9th Cir. 2018) ("AT&T').The courts and the FCC have expressed jurisdiction based on activity. In_the matter at hand-as an interconnected service provider-XCAST is a presumptive common carrier and that presumption in how XCast runs this part of its business.

63. The ITG has failed to inform its own dues-paying members about the analytics being developed from data they are provided, who has access to the information, what (criteria) the ITG applies to detemiined something is "suspicious" or how their analytics are brought to bear by whom on that question.

64. The ITG has also withheld any information that might assist its members in identifying "bad actors." The ITG admits they know who the bad actors are. Failure to share this information has created an atmosphere of distrust and confusion among voice providers who have received no constructive guidance from anyone-even while being legally obligated to abide by the rules established by the Federal Communications Commission.

65. This means that the ITG and the federal government continue to rely on bulk metadata to actively pursue thousands of American small businesses voice providers while intentionally ignoring the two dozen criminals who are actually committing the fraud.[9] Based on highly reliable sources, my information and belief is:

- All forms of fraud were becoming rampant on all communications platforms. Private industry fraud teams-prior to the establishment of the ITG--began working as a cooperative team as early as 2015 to see how they could jointly track down criminals at the source through sophisticated IP address analyses. By 2020, their joint investigations were able to conclusively confirm that over 90% of illegal calls were being originated from outside the country. These Big Tech private sector fraud team's collective data mining tools allowed them to look up IP addresses and identify by packets the exact mapping of how information was sent to their global networks or through intermediaries. US policy makers are well aware of this but have continued to embrace the view-and spread the lie--that thousands of people are committing phone fraud when in fact the fraud is work of only a handful of criminal cartels.

- Big Tech fraud groups are able to perform very complex tracebacks. If their networks received a voice call, they can reverse the signal and identify the media packet directly to the source. They then pinpointed the criminals without analyzing the chain of carriers. Long ago their data-mining sophistication allowed them to determine that

illegal robo calls were not coming from "criminal call centers" but from a remote servers that can easily be identified by law enforcement.[10] (This information has been circulating around within the middle-management groups of the US Telecom, FTC, FCC and selected state Attorneys General offices for several years-with apparently no oversight, direction or coordination from senior policy makers.)

- In July 2020 this private industry "Strike Force"-which included fraud teams from AT&T, Microsoft, Google--assembled in the offices of Attorney General Barr in July 2020 and identified the dozen individuals-by name and address-in India [11]who were responsible for over 90% of the illegal calls. Attorney General Barr was initially skeptical that DOJ could do anything due to certain extradition treaties but became persuaded he should appoint a Doja task force coordinator within the Civil Division (which has no criminal prosecutorial authorities.) The individual originally appointed by AG Barr moved to another job and the post remained vacant for a long period.

- On June 17, 2021, private industry fraud groups held meetings in New Delhi at the US Embassy that involved the FBI, CIA and Indian Intelligence communities. The Indian law enforcement community indicated their willingness to track down the criminals if the US would be willing to identify them through the remote servers.

- Eighteen months later-on January 23, 2023-a DOJ readout revealed that the group had not met since October 2021. During their January 2023 meeting the parties posed for pictures and *"reaffirmed their mutual commitment to continued cooperation in addressing dynamic and evolving crimes by building upon the experience gained through recent efforts and further re.fining processes for the exchange of information....."*

66. Meanwhile, internet-enabled criminals have altered their behavior. Despite some episodic declines, illegal robo-calling has not been dramatically reduced while other forms of fraud has been rapidly increasing. Identity theft is on the rise and already one's child could get a phone message and mistake an AI generated voice

---

lO These remote servers-in both the US and Western Europe--are leased by off-shore criminals. A remote server can place the outbound call to the potential victim and when the victim answers or hits "I" that message is conveyed back to the server where somebody is live on the phone and the server then directs the call to the next available "live person." The remote server must have an IP address in order to bring up the other side of the call. (This is how some Call Center ACDs works. XCAST's software does!!_Work that way; it can only make one simultaneous outbound call.)

11 Toe industry "Strike Force Group" ascertained that a US-based providers who is participating in these schemes can represent they do not engage in outbound calls but can then engage an Indian group who actually make the outbound calls for them and then "warm transfer" them back to the US. XCAST has never engaged in such a process. XCAST does not engage in any active marketing; two-person sales group manages relationships with independent Resellers and Agents representing hundreds of small to mid-size US businesses-including restaurants, national retail outlets, hotels, schools, local, state and federal government, law firms, hospitals, etc. Only a small portion of XCAST's PBX business revenue is initiated internally.

for their parent.

67. Emerging cartels are engaged in human trafficking--moving across Asia into Malayia, Thailand, Cambodia and Vietnam-where exploited (arguable kidnaped) people are deploying new technology and strategies by establishing call centers in remote areas. Cartels are exploiting social media and training people to "become friends" so that over time victims can be gradually groomed for a much bigger kill as they trust and follow their "new friend" down the bitcoin investment and traditional financial rat holes to steal everything with just one click.

68. On information and belief, and through my own knowledge and resources, US intelligence and law enforcement agencies are well aware of these trends. They also know about the reliance that international criminal cartels have on encrypted phones-the go-to lifeline for drug smuggling between Mexico, Netherlands, Greece and Albania. Although Europol has finally discovered how to penetrate the encryption, Europol cannot do anything without the resources the US government can bring to bear. The federal service is fully aware of this technology and criminal focus shift. The federal government has in hand every existing communication tracking and surveillance tool known to man. No reasonable person should assume a small company with less than two dozen employees can identify

criminals responsible for phone fraud. The federal government can **stop internet.-based crimes at the source** if they decide to stop "playing with their food" as Robert Mueller once described such delays for doing nothing.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 25th day of September, 2023.

;J

P?tricia Mathis