

Expert Rebuttal Report of  
Douglas C. Schmidt, Ph.D.

Public Redacted Version

**IN THE SUPERIOR COURT OF THE STATE OF ARIZONA**  
**IN AND FOR THE COUNTY OF MARICOPA**

STATE OF ARIZONA, <i>ex rel.</i> MARK	)	
BRNOVICH, Attorney General,	)	No. CV2020-006219
	)	
Plaintiff,	)	
	)	
v.	)	Assigned to the Hon. Timothy Thomason
	)	
GOOGLE LLC, A Delaware Limited	)	<b>(COMPLEX CALENDAR)</b>
Liability Company,	)	
	)	
Defendant.	)	
<hr/>		)

Expert Rebuttal Report of Douglas Craig Schmidt, Ph.D.

HIGHLY CONFIDENTIAL – ATTORNEYS’ EYES ONLY  
PURSUANT TO PROTECTIVE ORDER

Nashville, TN  
June 22, 2022

## I. Introduction

1. I, Douglas Craig Schmidt, previously submitted a report in this action on May 4, 2022 (my “Opening Report”). I have received and reviewed the Expert Reports of Drs. Zervas and Steckel. I am submitting this report to respond to certain of the opinions and conclusions in those reports.

## II. Rebuttal to the Expert Report of Dr. Zervas

2. Dr. Zervas states that Dr. Nielson’s claim that “[w]hen a consumer purchases an Android device, he or she receives a device that Google uses to track that user’s location” is a misleading description of what Android devices are.<sup>1</sup> However, his explanation of what constitutes an Android device directly supports Dr. Nielson’s claim. In particular, Dr. Zervas states that “an Android device is configured to satisfy users’ mobile communication needs and support multiple aspects of modern life that rely on mobile communication via broadband, *including location services*.”<sup>2</sup> Location services are precisely what Android devices provide that Google uses to track a user’s location, so Dr. Zervas’s statement that Dr. Nielson’s claim is “a misleading description of what Android devices are” is contradicted by his own opinion.

3. Dr. Zervas also alleges that “the details of the experiment described in Dr. Schmidt’s 2018 Technical Report are not transparent with respect to the settings and specifics of the software used and thus it is not often clear, for example, if data are collected by the Android device or a Google application or by a third party application.”<sup>3</sup> I disagree with Dr. Zervas’s allegation since Appendix D of my 2018 Study explains my method for location traffic monitoring in detail. In particular, Appendix D explains that “In specific cases, requests to Google were further decoded to analyze the information that was passed at a more granular level. One specific request to Google that was further decoded was the

---

<sup>1</sup> June 8, 2022 Expert Report of Georgios Zervaz, Ph.D., ¶ 161.

<sup>2</sup> June 8, 2022 Expert Report of Georgios Zervaz, Ph.D., ¶ 161 (emphasis added).

<sup>3</sup> June 8, 2022 Expert Report of Georgios Zervaz, Ph.D., ¶ 162.

“Google location API,” designated by the /loc/m/api endpoint. The location specifications were reverse engineered by removing the message header and decoding the compressed protobuf message. The decoded location API contained Wi-Fi and network scans that were used to determine the location of the device.”<sup>4</sup>

4. Dr. Zervas states that “From what I have seen, his 2018 Technical Report does not cover or even mention IPGeo and [REDACTED], and Dr. Schmidt provides no explanation for how the 2018 Technical Report relates to those services.”<sup>5</sup> As I noted in my Opening Report, the Nielson Declaration indicates that Google’s IPGeo service uses [REDACTED].<sup>6</sup> As I explained in my Opening Report, my 2018 Study supports the conclusion in the Nielson Declaration that [REDACTED].<sup>7</sup> My 2018 Study supports that [REDACTED], which in turn supports Dr. Nielson’s conclusions that [REDACTED].<sup>8</sup> Moreover, I noted in my 2018 Study that Google could obtain a “coarse location” though a network’s IP Address, which could be further refined using “nearby WiFi access points.”<sup>9</sup>

5. It is true that Dr. Nielson’s declaration, report and referenced materials expose Google’s IPGeo and [REDACTED] services in some ways that I did not know (and could not have known). Dr. Nielson cites extensive internal materials and deposition testimony that were produced by Google under Protective Order and were obviously unavailable to me when I conducted my study in 2018. For example, Dr. Nieson’s declaration references an internal Google document where an engineer explains that [REDACTED]

---

<sup>4</sup> Schmidt 2018 Study, ¶129.

<sup>5</sup> June 8, 2022 Expert Report of Georgios Zervaz, Ph.D., ¶ 163.

<sup>6</sup> Opening Report, at ¶ 49.

<sup>7</sup> Opening Report, at ¶ 50.

<sup>8</sup> Opening Report, at ¶ 51.

<sup>9</sup> Schmidt 2018 Study, ¶17.

[REDACTED]<sup>10</sup> The Google engineer also explained (as quoted by Dr. Nielson) that Google [REDACTED]

[REDACTED]<sup>11</sup> Obviously, that information is not something I knew—or could have known—when conducting my 2018 Study.

### **III. Rebuttal to Expert Report of Dr. Steckel**

6. Dr. Steckel states that “The Schmidt 2018 Study, as it relates to an ‘average user’s daily activities using an Android mobile phone device,’ cannot be used as a means to reliably and scientifically draw conclusions about a broader user population.”<sup>12</sup> I disagree with Dr. Steckel’s opinion. One of the key points of my 2018 Study was that Google designs its products and services to collect a significant amount of data passively via an Android device, i.e., without any interaction from the user.<sup>13</sup> Passive data collection is not necessarily dependent on the user’s activities on a particular day. The results of my 2018 Study therefore *do* generalize to the broader population who own Android devices since their devices are programmed to collect this information without user involvement or knowledge of user activities.

7. Moreover, Dr. Steckel provides no evidence that the Google data collection results from my 2018 Study are inaccurate nor does he present any evidence that these results are not representative of an “average user's daily activities.” In fact, I have not seen anything from Google challenging the accuracy of my study results or disputing that results can be generalized more generally to Android users. As far I can tell, Dr. Steckel does not purport to have any training or expertise in computer science, so it is not clear to me what basis he would have to contest the substance of my study.

---

<sup>10</sup> November 16, 2021 Declaration of Seth Nielson, at ¶ 118.

<sup>11</sup> November 16, 2021 Declaration of Seth Nielson, at ¶ 117.

<sup>12</sup> June 8, 2022 Expert Rebuttal Report of Joel H. Steckel, Ph.D., at ¶ 52.

<sup>13</sup> Schmidt 2018 Study, Section III.C.

8. Dr. Steckel also states that “this account has Location History turned on, which I understand results in data collected in the study not being reflective of the scenario at issue in this case where Location History is off and WAA is on.”<sup>14</sup> My understanding of the State’s case, however, is that it is much broader than just Google’s deceptive disclosure as it relates to WAA collecting location data when Location History is off.<sup>15</sup> As I explained in my Opening Report, my 2018 Study measures the extent of Google’s data collection.

June 22, 2022  
Nashville, TN



---

Douglas Craig Schmidt, Ph.D.

---

<sup>14</sup> June 8, 2022 Expert Rebuttal Report of Joel H. Steckel, Ph.D., at ¶ 53.

<sup>15</sup> Opening Report, at ¶¶ 25-29.