

September 28, 2020

Kate Wasch, Esq.  
Chief Counsel, Employment & Litigation  
Office of Legal Affairs  
Georgia Institute of Technology  
760 Spring Street NW, Suite 324  
Atlanta, Georgia 30332-0495

Dear Kate:

Thank you for your response to our inquiry whether Georgia Tech would agree to pay for David Dagon's legal fees with respect to the investigation being conducted by a D.C. grand jury on behalf of Connecticut United States Attorney John Durham ("the Durham investigation"). You state in your reply that:

It is not clear to me that the work David did was undertaken in his role as a GT employee. He may have used data to which he had access by virtue of his employment at GT, but the work was not part of his GT duties."

We hope, via this letter, to clarify any confusion regarding Georgia Tech's and Mr. Dagon's role and whether Mr. Dagon's actions were undertaken within the scope of Mr. Dagon's employment for Georgia Tech.

### Background

At the outset, we note that Mr. Dagon was, at all relevant times, employed as a Research Scientist by Georgia Tech, specifically to conduct research and obtain funding in the areas of Internet attribution, IoT devices, and DNS research. Your own policies indicate that research faculty's "primary job responsibility involves leading, developing, and delivering the research, extension, and technology transfer programs of the Institute."

<http://policylibrary.gatech.edu/faculty-handbook/2.3.1-members-0>

This is precisely what Mr. Dagon has done in his job performance during his employment at Georgia Tech.

Mr. Dagon's work for Georgia Tech included the attribution work he did on the Mariposa botnet, for which Mr. Dagon received an award and commendation from then FBI Director Mueller, and for which the University released several press releases. In addition, Georgia Tech presented Mr. Dagon with an exceptional award for "Outstanding achievement in research program development, for initiating team research to create a new thought leadership platform during the period of January 2012 to December 2014." The award was accompanied by a generous cash

payment. Georgia Tech presented Mr. Dagon with yet another of these rarely bestowed awards for “Initiating team research to create a new thought leadership platform during the period January 1, 2015 to December 31, 2017” – *the exact period of time that is being examined by the Durham investigation.*

#### Work Performed by Mr. Dagon for Georgia Tech That is Subject to the Investigation

The work that Mr. Dagon did on attribution analysis of communications traffic, which relates to the current legal matter, involved research on the Democratic National Convention hack, the Advanced Persistent Threat-28 (APT-28) malware, analysis of potential attack traffic related to the 2016 election (including traffic between the Trump Organization, Spectrum Health, and Alfa Bank), and analysis of Yota phone communications traffic. This work is no less within the scope of Mr. Dagon’s employment than the work he did on the Mariposa botnet.

Indeed, much of this work was done in preparation for and in fulfillment of the obligations of the multi-million-dollar DARPA contract he helped bring to Georgia Tech (and about which the University similarly issued a press release). To suddenly decide that this attribution work was “not within the scope of Mr. Dagon’s employment” would, of course, put this funding at risk, and would similarly implicate any remedies or defenses the University may have under O.C.G.A. 50-21-25, not only with respect to the Durham investigation, but generally. In short, Mr. Dagon’s attribution research was not a frivolous pursuit, but was integral to the research he secured for Georgia Tech. Any assertion to the contrary is disingenuous.

As we noted in our previous call, when Mr. Dagon undertook a thorough review of work related to the investigation, which was performed from the end of 2016 forward, *he discovered that almost all of the initial work performed by him was on behalf of Georgia Tech under the DARPA contract: the work related to queries submitted by the U.S. Department of Justice (DOJ) through DARPA regarding Russian communications between Alfa Bank and the Trump organization and Mr. Trump’s use of a Russian Yota phone — the exact subject matter of the criminal Grand Jury subpoena that Mr. Dagon received from the Durham investigation.* The requests were sufficient to require Mr. Dagon and Prof. Antonakakis (“Manos”) to set up a file within the DARPA project called “DOJ” and a sub file called “Mueller” because they knew that these requests were coming from DOJ and being sent back (via DARPA) to DOJ and the Mueller investigation.

This is precisely what the Durham investigators are looking at – the work Mr. Dagon did under the DARPA contract on behalf of Georgia Tech. In particular, the research that Mr. Dagon conducted on DNS records starting in late 2016 and continuing through early 2017, and the research he conducted related to the Yota phone were always conducted as part of Mr. Dagon’s duties as a security researcher employed by Georgia Tech.

This work was in furtherance of his duties and obligations at Georgia Tech; it was for the benefit of Georgia Tech; and it was within the scope of his employment at Georgia Tech. In addition, his response to first the FBI/DOJ inquiries that were made through DARPA, and his later response to the grand jury subpoena and other investigative queries have always been within the scope of his employment and meticulously coordinated with his employer.

All of the initial meetings and discussions that Mr. Dagon held among security researchers and Internet service providers (ISPs) about the data that Georgia Tech would need to create a database for the analysis of DNS records and the methods that Mr. Dagon would use to analyze DNS records (not just related to the Trump Organization and Alfa Bank, but in general) were conducted on behalf of Georgia Tech. Indeed, Mr. Dagon's trip to the 2016 Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) meeting in Philadelphia, at which the initial discussions among researchers and ISPs took place regarding the DNC hack and analysis of traffic data, was a trip that was authorized and funded by Georgia Tech and was clearly within the scope of Mr. Dagon's employment.

Additionally, the queries against the database created under or in furtherance of the DARPA contract, including the specific queries made for or on behalf of the Department of Justice and/or its component agencies (including the FBI), as well as those made on behalf of the Department of Defense, were done as part of Mr. Dagon's work for Georgia Tech, and were within the scope of his employment. Mr. Dagon's work with respect to the Yota phones may also implicate grants that Mr. Dagon was instrumental in obtaining for Georgia Tech from other entities like the National Institutes of Standards and Technology (NIST), which related to the analysis of signatures and behavior of certain Internet of Things (IoT) devices. This was research for which Mr. Dagon was responsible for bringing in funds for Georgia Tech, and his associated research was conducted within the scope of Mr. Dagon's employment.

While Georgia Tech did not direct any specific inquiry or report, Mr. Dagon's DNS research in general – and the specific inquiries and analysis which are the subject of the Durham grand jury probe – are, and have always been, part of Mr. Dagon's work on behalf of Georgia Tech. Indeed, Georgia Tech benefits from – and has always benefited from – Mr. Dagon's work, as well as from the tremendous prestige, capabilities, and funding that Mr. Dagon has brought to Georgia Tech as a result of his world renown expertise and research, which are reflected in the award of the DARPA contract and the research which is the subject of the grand jury investigation.

This research is not something that Mr. Dagon undertook as a “frolic and detour” or for private commercial advantage. Indeed, as we discussed, even Mr. Dagon's use of the commercial entity “Glomar Research” was to conveniently purchase certain hardware for Georgia Tech research on behalf of the DARPA contract and his employer. Importantly, Mr. Dagon kept Manos and other officials at Georgia Tech apprised of his work, his research plans, and findings. There were ample opportunities for Georgia Tech to advise him during these months that this work was not something they wanted him to do or considered within the scope of employment. No one ever advised him of such. To the contrary, the insights gained from this work allowed Georgia Tech to select and price datasets for the DARPA project, making it all the more successful.

We have reviewed the DARPA contract that you provided (which was not the contract applicable to the DARPA work referenced in this letter), which lists Glomar Research as a subcontractor. This reinforces that Mr. Dagon's use of Glomar Research was not unrelated to his work for Georgia Tech and was done for the benefit of Georgia Tech.

Mr. Dagon has always treated his actions, both in conducting the research at issue and responding to the Durham investigation as being part of his responsibility as an employee of Georgia Tech. For example, on April 30, 2020, in an email to DOJ investigator Tim Fuhrman, following a conversation between Mr. Dagon and Fuhrman, Mr. Dagon stated:

“As we discussed, we’re required to work through the school’s liaison process. Prof. Manos Antonakakis, addressed above, is my co-PI on research projects and supervises my work in the lab....So can you briefly relay to Prof. Antonakakis the nature of your inquiry? He can then engage our university and federal liaison staff. You noted this concerns the general type of DNS information discussed in this public report:

[https://justthenews.com/sites/default/files/2020-04/Ankura\\_AlfaBank\\_Res=earchAnalysis\\_Apr2020dh.pdf.pdf.pdf](https://justthenews.com/sites/default/files/2020-04/Ankura_AlfaBank_Res=earchAnalysis_Apr2020dh.pdf.pdf.pdf)

...I suspect that your inquiry may be relevant to Georgia Tech, and our sponsored research projects.”

Clearly, in responding to the Durham investigation – the precise matter for which Mr. Dagon seeks reimbursement of legal fees – Mr. Dagon was acting as an employee of Georgia Tech and was deferring to his employer. A subsequent email from Manos to Mr. Dagon on June 16, 2020, stated:

“Just talked to the Dean and the consensus at GT is that we will not be doing anything to help DoJ unless legal documents are presented to us. GT legal will handle any subpoenas arriving to my or your mail boxes on this topic because they consider it a work-related issue. Both the GT lawyers and/or the local FBI folks are under the impression that subpoenas will not arrive to us because if DoJ wanted to reach that point they would have already.... We are under very strict communication guidelines when it comes to this issue. You do not talk to the DoJ investigator without the presence of a GT lawyer on the line. You forward to me and the Chief of Police any new communication requests from DoJ in this subject and you do not correspond with them unless GT legal asks you to.”

On July 6, 2020, Manos sent an email to you and Ling-Ling and stated:

“Hey Kate and Ling-Ling, Dave is looking for some advice. Can we please provide some guidance to our researcher on how he should reply back to the DoJ investigator?”

In sum, Mr. Dagon’s entire response to the Durham investigation has been coordinated with your office, and has been as an agent and representative of Georgia Tech. His seeking and obtaining private counsel were within his personal right and with the intention to minimize unwanted publicity or attention to Georgia Tech. The fact that the issues being investigated by the Durham prosecutors are wholly without merit – both factually and legally – enhance the argument that Mr. Dagon’s lawful research was within the scope of his employment, and his response to the investigation is similarly within that scope.

Indeed, it was for this reason that we both agreed that a representative of your office should be present if Mr. Dagon decided to present evidence to the Durham investigators, and that any statements he made would be as a representative of his employer. Thus, Mr. Dagon's work which is the subject of the Durham investigation, his response to subpoenas, and his response to the Durham investigation in its entirety is work performed within the scope of Mr. Dagon's employment at Georgia Tech.

#### Mr. Dagon's Request for Legal Fees

Mr. Dagon's request for the university to pay his legal fees associated with this matter is not out of the ordinary. Prof. L. Jean Camp of Indiana University, for example, who has received a subpoena for the criminal grand jury investigation and the pending civil litigation filed by Alfa Bank, is being represented by counsel paid for by the university. Similar action is not without precedent in Georgia.

O.C.G.A. § 45-9-21(c) provides an example of a statute which permits a public entity to reimburse a government employee the costs and expenses associated with responding to criminal investigations that arise within the scope of their employment. *Bd. of Comm'rs v. Saba*, 278 Ga. 176, 598 S.E.2d 437 (2004)

In other cases, Georgia Courts have held that government agencies either had the authority to, or the legal requirement to, reimburse employees' legal expenses if those expenses were incurred in connection with their duties as government employees. Accord, *Gwinnett Cty. v. Blaney*, 275 Ga. 696, 572 S.E.2d 553 (2002) (espousing the general rule that the legal expenses of a government employee should be reimbursed if the employee was acting within the scope of their employment).

As the Court noted in *Heiskell v. Roberts*, 342 Ga. App. 109, 109, 802 S.E.2d 385, 387 (2017) "when "an official, acting in his official capacity, is required to hire outside counsel to assert a legal position the local government attorney ... will not assert, and the official is successful in asserting his or her position, the local government must pay the official's attorney fees." *Gwinnett County v. Yates*, 265 Ga. 504, 508 (2) (458 SE2d 791) (1995). "This is not because of any bad faith or improper conduct on the part of the local government, in this case, the county. Rather, attorney fees in this instance are simply an expense of government operation." *Gwinnett Cty. v. Yates*, 265 Ga. 504, 508-09, 458 S.E.2d 791, 795 (1995)

In this instance, it is doubtful that either Georgia Tech counsel or the Georgia Attorney General would be capable of representing Mr. Dagon in connection with the Durham investigation due to issues of privilege, waiver, and information sharing inherent in the nature of the Durham investigation. The Attorney General would be put in the untenable position, as a law enforcement entity, of having to assert Mr. Dagon's right not to testify before a federal grand jury – the assertion of which right could rightly serve the interests of Georgia Tech. Thus, it serves the interests of Georgia Tech and the State to have Mr. Dagon represented by private counsel with the concomitant authority to assert certain privileges which might be waived with representation provided by the Attorney General.

It is also important to note that should Georgia Tech assert that Mr. Dagon's work within the scope of the investigation was not within the scope of his employment, there might be serious,

adverse consequences in the event that Georgia Tech is civilly sued by entities like Alfa Bank, which has already filed two civil “John Doe” lawsuits in Florida and Pennsylvania. Alfa Bank has issued dozens of subpoenas to individuals (including to numerous cybersecurity researchers) and institutions in an effort to attach institutions and names to the various “John Doe’s” in the complaint. A position that Mr. Dagon was not acting as an employee of the State might be used to vitiate any immunity that Georgia Tech could otherwise assert in a civil case, and such a position is inconsistent with the facts. Mr. Dagon was and is an employee of Georgia Tech with the responsibility of researching precisely the kind of activities he had undertaken.

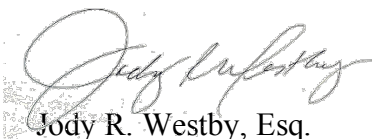
We are happy to address any concerns that you may have in this regard, but it seems clear to us that a person employed as a security researcher who conducts security research for his employer, and also brings millions of dollars in research grants to the school from this research, is acting within the scope of his employment in doing so. We hope this information clarifies the issue and that Georgia Tech will agree to assume responsibility for his legal fees.

Per our earlier discussion, we have attached a draft Third Party Payor Agreement, which is commonly used when an employer assumes responsibility for legal fees of one of its employees. Thank you for your attention to this matter. We look forward to your response.

Yours truly,



Mark D. Rasch, Esq.  
Admitted in NY MA MD



Jody R. Westby, Esq.  
Admitted in DC, PA, CO