

Exhibit 1

Sussmann, Michael A. (Perkins Coie)

From: Sussmann, Michael A. (Perkins Coie)
Sent: Thursday, October 13, 2016 3:43 PM
To: Chan, Elvis M. (SF) (FBI)
Cc: Rich, Patricia R. (SF) (FBI); Newell, Sean (NSD) (JMD); Hawkins, E. A. (WF) (FBI); Sills, Jonathan P. (OGC) (FBI); Hooper, Joseph M. (CYD) (FBI); Cheeks II, James E. (CYD) (FBI); Milligan, Julissa L. (Perkins Coie)
Subject: Re: Follow Up

In theory, sure, but I'm checking to see if the data is with CrowdStrike now or at the DNC.

I'll start a new email and put you directly in touch with CrowdStrike.

Michael Sussmann | Perkins Coie LLP

P: 202.654.6333

www.perkinscoie.com/msussmann

From: "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>
Date: Thursday, October 13, 2016 at 2:55 PM
To: Michael <msussmann@perkinscoie.com>
Cc: "Rich, Patricia R. (SF) (FBI)" <Patricia.Rich@ic.fbi.gov>, "Newell, Sean (NSD) (JMD)" <Sean.Newell@usdoj.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, Jonathan Sills <Jonathan.Sills@ic.fbi.gov>, "Hooper, Joseph M. (CYD) (FBI)" <Joseph.Hooper@ic.fbi.gov>, "Cheeks II, James E. (CYD) (FBI)" <James.Cheeks@ic.fbi.gov>, "Milligan, Julissa L. (WDC)" <JMilligan@perkinscoie.com>
Subject: RE: Follow Up

Hi Michael,

Do you believe DNC/DCCC would be amenable to letting FBI computer forensics personnel onsite to conduct the imaging?

Regards,

Elvis

=====

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division
Federal Bureau of Investigation
Work: 415-553-7605
Cell: **REDACTED**-6196
E-mail: elvis.chan@ic.fbi.gov

From: Sussmann, Michael A. (Perkins Coie) [<mailto:MSussmann@perkinscoie.com>]
Sent: Thursday, October 13, 2016 10:58 AM
To: Chan, Elvis M. (SF) (FBI) <Elvis.Chan@ic.fbi.gov>

SCC_0000696

Cc: Rich, Patricia R. (SF) (FBI) <Patricia.Rich@ic.fbi.gov>; Newell, Sean (NSD) (JMD) <Sean.Newell@usdoj.gov>; Hawkins, E. A. (WF) (FBI) <Adrian.Hawkins@ic.fbi.gov>; Sills, Jonathan P. (OGC) (FBI) <Jonathan.Sills@ic.fbi.gov>; Hooper, Joseph M. (CYD) (FBI) <Joseph.Hooper@ic.fbi.gov>; Cheeks II, James E. (CYD) (FBI) <James.Cheeks@ic.fbi.gov>; Milligan, Julissa L. (Perkins Coie) <JMilligan@perkinscoie.com>
Subject: Re: Follow Up

Elvis,

Here's the information from CrowdStrike:

The images requested by the FBI are approx. 3.1 TB of data. Pulling, encrypting, and transferring the data, and shipping the drives will require approx. 10 hours of labor. plus associated expenses.

Our clients are paying \$375/hr = \$3,750 in fees.
Add approx \$140 for the drive to which images will be transferred.
Add shipping rates.
And we're looking at around \$4,000.00

(There are no legal fees from my firm incorporated into this estimate — it's just the time, materials and incidental costs for CrowdStrike.)

Please advise.

Michael

Michael Sussmann | Perkins Coie LLP

P: 202.654.6333

www.perkinscoie.com/msussmann

From: "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>
Date: Thursday, October 13, 2016 at 1:06 PM
To: Michael <msussmann@perkinscoie.com>, "Rich, Patricia R. (SF) (FBI)" <Patricia.Rich@ic.fbi.gov>, "Newell, Sean (NSD) (JMD)" <Sean.Newell@usdoj.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, Jonathan Sills <Jonathan.Sills@ic.fbi.gov>, "Hooper, Joseph M. (CYD) (FBI)" <Joseph.Hooper@ic.fbi.gov>, "Cheeks II, James E. (CYD) (FBI)" <James.Cheeks@ic.fbi.gov>
Cc: "Milligan, Julissa L. (WDC)" <JMilligan@perkinscoie.com>
Subject: RE: Follow Up

Michael,

Can you let us know what the hourly rate/total cost would be? I need to follow up with FBIHQ. Thanks.

Regards,
Elvis

=====

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division

SCC_0000697

Federal Bureau of Investigation
Work: 415-553-7605
Cell: REDACTED-6196
E-mail: elvis.chan@ic.fbi.gov

----- Original message -----

From: "Sussmann, Michael A. (Perkins Coie)" <MSussmann@perkinscoie.com>
Date: 10/12/2016 5:58 PM (GMT-08:00)
To: "Rich, Patricia R. (SF) (FBI)" <Patricia.Rich@ic.fbi.gov>, "Newell, Sean (NSD) (JMD)" <Sean.Newell@usdoj.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>
Cc: "Milligan, Julissa L. (Perkins Coie)" <JMilligan@perkinscoie.com>
Subject: Re: Follow Up

We already had the call, i.e., Adrian called me on Tuesday.

CrowdStrike has estimated that it will take 10 hours of work to get the responsive information that it has. Would the FBI be able to reimburse the DNC and DCCC for those costs?

Thanks.

Michael Sussmann | **Perkins Coie LLP**

P: 202.654.6333

www.perkinscoie.com/msussmann

From: "Rich, Patricia R. (SF) (FBI)" <Patricia.Rich@ic.fbi.gov>
Date: Tuesday, October 11, 2016 at 6:11 PM
To: "Newell, Sean (NSD) (JMD)" <Sean.Newell@usdoj.gov>, Michael <msussmann@perkinscoie.com>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>
Cc: "Milligan, Julissa L. (WDC)" <JMilligan@perkinscoie.com>, "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>, Leigh Nichols <LNichols@perkinscoie.com>
Subject: RE: Follow Up

Anytime Thursday works for me.
Thank you,
Patricia

From: Newell, Sean (NSD) [<mailto:Sean.Newell@usdoj.gov>]
Sent: Tuesday, October 11, 2016 2:19 PM
To: Sussmann, Michael A. (Perkins Coie) <MSussmann@perkinscoie.com>; Hawkins, E. A. (WF) (FBI) <Adrian.Hawkins@ic.fbi.gov>
Cc: Milligan, Julissa L. (Perkins Coie) <JMilligan@perkinscoie.com>; Chan, Elvis M. (SF) (FBI) <Elvis.Chan@ic.fbi.gov>; Nichols, Leigh (Perkins Coie) <LNichols@perkinscoie.com>; Rich, Patricia R. (SF) (FBI) <Patricia.Rich@ic.fbi.gov>
Subject: RE: Follow Up

Looping in Patricia Rich from San Francisco.

The afternoon is better for me. But, given what you say below, I'll just let Leigh coordinate a time with Patricia and Adrian. I'll then join if I am available.

SCC_0000698

Sean

From: Sussmann, Michael A. (Perkins Coie) [<mailto:MSussmann@perkinscoie.com>]
Sent: Tuesday, October 11, 2016 12:55 PM
To: Hawkins, E. A. (WF) (FBI); Newell, Sean (NSD)
Cc: Milligan, Julissa L. (Perkins Coie); Chan, Elvis M. (SF) (FBI); Nichols, Leigh (Perkins Coie)
Subject: Re: Follow Up

Adrian, I'm free now until 3:00 pm. If that doesn't work, since I'll be OOO tomorrow, please work with my assistant, Leigh, to set up a call. But this is not a big deal – just a status update – and I think I can easily relay it all to you. But your choice.

Michael Sussmann | **Perkins Coie LLP**

P: 202.654.6333

www.perkinscoie.com/msussmann

From: "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>
Date: Tuesday, October 11, 2016 at 11:48 AM
To: Michael <msussmann@perkinscoie.com>, "Newell, Sean (NSD) (JMD)" <Sean.Newell@usdoj.gov>
Cc: "Milligan, Julissa L. (WDC)" <JMilligan@perkinscoie.com>, "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>
Subject: RE: Follow Up

I'm checking with SF on their availability.

--

----- Original message -----

From: "Sussmann, Michael A. (Perkins Coie)" <MSussmann@perkinscoie.com>
Date: 10/11/2016 11:17 AM (GMT-05:00)
To: "Newell, Sean (NSD) (JMD)" <Sean.Newell@usdoj.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>
Cc: "Milligan, Julissa L. (Perkins Coie)" <JMilligan@perkinscoie.com>
Subject: Rc: Follow Up

Sean and Adrian,

Can you two get on a short call today with Julissa and me to discuss the status of your requests? We also can just get on the phone with Adrian. I will be OOO tomorrow, so if today doesn't work, let's shoot for Thursday.

Thanks,

Michael

Michael Sussmann | **Perkins Coie LLP**

P: 202.654.6333

www.perkinscoie.com/msussmann

SCC_0000699

From: "Newell, Sean (NSD)" <Sean.Newell@usdoj.gov>
Date: Tuesday, October 4, 2016 at 10:09 AM
To: Michael <msussmann@perkinscoie.com>
Cc: "Lai, Sarah (NSD)" <Sarah.Lai3@usdoj.gov>, "Shih, Jeffrey (USACAN)" <Jeffrey.Shih@usdoj.gov>, "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, "Milligan, Julissa L. (WDC)" <JMilligan@perkinscoie.com>
Subject: RE: Follow Up

Sounds good. Thank you!

From: Sussmann, Michael A. (Perkins Coie) [<mailto:MSussmann@perkinscoie.com>]
Sent: Monday, October 03, 2016 11:13 PM
To: Newell, Sean (NSD)
Cc: Lai, Sarah (NSD); Shih, Jeffrey (USACAN); Chan, Elvis M. (SF) (FBI); Hawkins, E. A. (WF) (FBI); Milligan, Julissa L. (Perkins Coie)
Subject: Re: Follow Up

Sean,

We certainly can share information with you on a rolling basis. We hope to have some information for you later in the week.

Regards,

Michael

Michael Sussmann | **Perkins Coie LLP**

P: 202.654.6333

www.perkinscoie.com/msussmann

From: "Newell, Sean (NSD)" <Sean.Newell@usdoj.gov>
Date: Monday, October 3, 2016 at 12:13 PM
To: Michael <msussmann@perkinscoie.com>
Cc: "Lai, Sarah (NSD)" <Sarah.Lai3@usdoj.gov>, "Shih, Jeffrey (USACAN)" <Jeffrey.Shih@usdoj.gov>, "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, "Milligan, Julissa L. (WDC)" <JMilligan@perkinscoie.com>
Subject: RE: Follow Up

Michael and Julissa,

Good morning. I see that there may be another release of documents this week, maybe as early as tomorrow. Accordingly, I thought I would take that as an opportunity to check in on the first requests below. Would it be possible to do a rolling production? Happy to discuss further, if necessary.

Thanks!

Sean

SCC_0000700

From: Newell, Sean (NSD)
Sent: Tuesday, September 27, 2016 6:14 PM
To: MSussmann@perkinscoie.com
Cc: Lai, Sarah (NSD); Shih, Jeffrey (USACAN) (Jeffrey.Shih@usdoj.gov); Chan, Elvis M. (SF) (FBI) (Elvis.Chan@ic.fbi.gov); Hawkins, E. A. (WF) (FBI) (Adrian.Hawkins@ic.fbi.gov)
Subject: Follow Up

Michael,

As discussed yesterday, I am writing to request an initial batch of items from your clients. For all victims, DOJ and FBI request the following:

1. Any released files that are believed to be fake or modified and, if applicable, the original, unmodified file; and
2. 24-36 released files that were not circulated outside each of victim organizations (e.g., the donor list that was mentioned during our meeting) and a preliminary indication as to whether any of these may have been modified.

For DCCC only, we request access to data and/or employees that could speak to the two screenshots at the bottom of this e-mail as having been created from an amalgamation of files or directories on the DCCC network. We believe that DCCC and/or Crowdstrike may have looked into these screenshots between on or about September 2 and 6, 2016.

Finally, as Sarah mentioned during the meeting, some media reporting referred to an ongoing DNC effort to review documents to see if any had been "forged." To close the loop on that, we pulled up the following from a USA Today article regarding the September 13, 2016 information release: "In response to that most recent leak, DNC interim chair Donna Brazile [stated that their](#) 'legal team is now in the process of reviewing these private documents, and attempting to confirm their authenticity, as it is common for Russian hackers to forge documents.'"

We'll provide the more comprehensive wish list by the end of the week.

Thank you.

Sean Newell
Deputy Chief – Cyber
Counterintelligence and Export Control Section
National Security Division
U.S. Department of Justice
(202) 532-4585

Screenshot 1
<< OLE Object: Picture (Device Independent Bitmap) >>

Screenshot 2
<< OLE Object: Picture (Device Independent Bitmap) >>

SCC_0000701

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

SCC_0000702

Exhibit 2

Sills, Jonathan P. (OGC) (FBI)

From: Sills, Jonathan P. (OGC) (FBI)
Sent: Thursday, October 13, 2016 4:28 PM
To: Cheeks II, James E. (CYD) (FBI); Hooper, Joseph M. (CYD) (FBI); Nail, Michael A. (WF) (FBI)
Cc: Vanderstelt, Eric M. (CYD) (FBI)
Subject: RE: DNC / DCCC data

Good job!

From: Cheeks II, James E. (CYD) (FBI)
Sent: Thursday, October 13, 2016 4:26 PM
To: Hooper, Joseph M. (CYD) (FBI) <Joseph.Hooper@ic.fbi.gov>; Nail, Michael A. (WF) (FBI) <Michael.Nail@ic.fbi.gov>; Sills, Jonathan P. (OGC) (FBI) <Jonathan.Sills@ic.fbi.gov>
Cc: Vanderstelt, Eric M. (CYD) (FBI) <Eric.Vanderstelt@ic.fbi.gov>
Subject: Fwd: DNC / DCCC data

FYSA

--

----- Original message -----

From: "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>
Date: 10/13/2016 4:24 PM (GMT-05:00)
To: Justin Weissert <justin.weissert@crowdstrike.com>, "Sussmann, Michael A. (Perkins Coie)" <MSussmann@perkinscoie.com>, Ryan McCombs <ryan.mccombs@crowdstrike.com>
Cc: "Cheeks II, James E. (CYD) (FBI)" <James.Cheeks@ic.fbi.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, Shawn Henry <shawn@crowdstrike.com>, "Rich, Patricia R. (SF) (FBI)" <Patricia.Rich@ic.fbi.gov>
Subject: RE: DNC / DCCC data

Hi Justin,

FBI San Francisco greatly appreciates your help. Please send via FedEx (or other carrier with computer tracking) to:

Federal Bureau of Investigation
450 Golden Gate Avenue, 13th Floor
San Francisco, CA 94102
ATTN: SA Patricia Rich

Telephone: 415-553-7400

Regards,

SCC_0002762

Elvis

=====

Elvis M. Chan
Supervisory Special Agent
Squad CY-1
San Francisco Division
Federal Bureau of Investigation
Work: 415-553-7605
Cell: [REDACTED]-6196
E-mail: elvis.chan@ic.fbi.gov

From: Justin Weissert [mailto:justin.weissert@crowdstrike.com]
Sent: Thursday, October 13, 2016 1:20 PM
To: Sussmann, Michael A. (Perkins Coie) <MSussmann@perkinscoie.com>; Ryan McCombs <ryan.mccombs@crowdstrike.com>
Cc: Chan, Elvis M. (SF) (FBI) <Elvis.Chan@ic.fbi.gov>; Cheeks II, James E. (CYD) (FBI) <James.Cheeks@ic.fbi.gov>; Hawkins, E. A. (WF) (FBI) <Adrian.Hawkins@ic.fbi.gov>; Shawn Henry <shawn@crowdstrike.com>
Subject: Re: DNC / DCCC data

Hi Michael,

Thank you for the note. As we just discussed under a separate email thread, CrowdStrike wants to assist with this effort and, given the nature of the past activities and our commitment to supporting our friends at the FBI, we're going to move ahead with providing the information at no additional expense to anyone.

Our team is in the process of gathering this data now and we'll just need to know where the FBI would like this data to be sent. Agents Chan, Cheeks, and Hawkins, can you please let us know? Ryan McCombs will coordinate delivery from our end.

Thank you,
Justin

Justin J. Weissert

From: "Sussmann, Michael A. (Perkins Coie)" <MSussmann@perkinscoie.com>
Date: Thursday, October 13, 2016 at 3:45 PM
To: Ryan McCombs <ryan.mccombs@crowdstrike.com>, Justin Weissert <justin.weissert@crowdstrike.com>
Cc: "Chan, Elvis M. (SF) (FBI)" <Elvis.Chan@ic.fbi.gov>, "Cheeks II, James E. (CYD) (FBI)" <James.Cheeks@ic.fbi.gov>, "Hawkins, E. A. (WF) (FBI)" <Adrian.Hawkins@ic.fbi.gov>, Shawn Henry <shawn@crowdstrike.com>
Subject: DNC / DCCC data

Ryan and Justin,

Regarding the FBI requests under discussion, I have copied Agents Chan, Cheeks and Hawkins. They are asking whether FBI computer forensics personnel can come "onsite" to conduct the imaging. I'm not clear in this context what "onsite" means, i.e., is the data with you or with the DNC and DCCC? So I am connecting CrowdStrike and the Bureau to discuss directly on this email chain.

Thanks,

SCC_0002763

Michael

Michael Sussmann | Perkins Coie LLP

P: 202.654.6333

www.perkinscoie.com/msussmann

NOTICE: This communication may contain privileged or other confidential information. If you have received it in error, please advise the sender by reply email and immediately delete the message and any attachments without copying or disclosing the contents. Thank you.

CONFIDENTIALITY NOTE: This e-mail and any attachments are confidential and may be legally privileged. If you are not the intended recipient, do not disclose, copy, distribute, or use this email or any attachments. If you have received this in error please let the sender know and then delete the email and all attachments.

SCC_0002764

Exhibit 3

From: Abdallah, Chaouki T <ctabdallah@gatech.edu> on behalf of Abdallah, Chaouki T
Sent on: Monday, September 13, 2021 4:23:29 PM
To: McLaughlin, Steven W <sm140@gatech.edu>; Antonakakis, Manos <manos@gatech.edu>
CC: Keromytis, Angelos D <angelos@gatech.edu>
Subject: Re: As the dust slowly settles

Ditto...

Chaouki T Abdallah
Professor of Electrical & Computer Engineering
Executive Vice President for Research
Georgia Institute of Technology
EA: Lisa Tuttle, ltuttle@gatech.edu, 404-894-8884

From: McLaughlin, Steven W <sm140@gatech.edu>
Date: Monday, September 13, 2021 at 11:11 AM
To: Antonakakis, Manos <manos@gatech.edu>, Abdallah, Chaouki T <ctabdallah@gatech.edu>
Cc: Keromytis, Angelos D <angelos@gatech.edu>
Subject: Re: As the dust slowly settles

11a Sat works for me

Steve McLaughlin
Provost and Executive Vice President for Academic Affairs
Georgia Institute of Technology

From: "Antonakakis, Manos" <manos@gatech.edu>
Date: Monday, September 13, 2021 at 9:47 AM
To: "Abdallah, Chaouki T" <ctabdallah@gatech.edu>
Cc: "McLaughlin, Steven W" <swm@gatech.edu>, "Keromytis, Angelos D" <angelos@gatech.edu>
Subject: Re: As the dust slowly settles

Available all morning, but let's see if 11.00am works for everyone.

Manos

From: Abdallah, Chaouki T <ctabdallah@gatech.edu>
Date: Monday, September 13, 2021 at 9:46 AM
To: Antonakakis, Manos <manos@gatech.edu>
Cc: McLaughlin, Steven W <swm@gatech.edu>, Keromytis, Angelos D <angelos@gatech.edu>
Subject: Re: As the dust slowly settles

Please suggest a time...

Chaouki T. Abdallah
Professor of Electrical & Computer Engineering
Executive Vice President for Research
Georgia Institute of Technology

On Sep 13, 2021, at 09:39, Antonakakis, Manos <manos@gatech.edu> wrote:

Absolutely, Steve. Not only I am available, but I am happy to make my patio/living room (the weather does look like rain) available.

Thanks, Manos

From: McLaughlin, Steven W <sm140@gatech.edu>
Date: Monday, September 13, 2021 at 9:05 AM

To: Antonakakis, Manos <manos@gatech.edu>, Abdallah, Chaouki T <ctabdallah@gatech.edu>, Keromytis, Angelos D <angelos@gatech.edu>
Subject: Re: As the dust slowly settles

Hi Manos

Great to hear from you - any chance we could meet in person with Chaouki and me on Saturday morning?

Best

Steve

Steve McLaughlin

Provost and Executive Vice President for Academic Affairs

Georgia Institute of Technology

From: "Antonakakis, Manos" <manos@gatech.edu>

Date: Friday, September 10, 2021 at 10:51 AM

To: "McLaughlin, Steven W" <swm@gatech.edu>, "Abdallah, Chaouki T" <ctabdallah@gatech.edu>, "Keromytis, Angelos D" <angelos@gatech.edu>

Subject: As the dust slowly settles

Hey Steve and Chaouki,

As the dust slowly settles, and everybody gets a very clear picture of this situation we will need to think about how we move forward.

In meetings I had with both of you, and as I originally identified with this email, we need to come up with a plan that describes how this research can continue in GT yet eliminate as much of the fly-by risk from all parties involved. From what took place over the last two months one thing is clear in my mind; I cannot keep doing things the way we have been doing them at GT. I love GT dearly, I have made numerous personal and financial sacrifices for GT, but the risk is simply too high for me. As Chaouki also acknowledged in one of our recent meetings, the risk is getting too high for GT as well. Not because we are doing something illegal --- it is just the nature of the attribution research our team is engaged in.

In my mind I see a single realistic path forward. The riskiest components of this entire research area (namely; commercial data acquisition and data access) will have to be moved outside GT with the explicit blessing of GT. Decoupling certain research areas from top schools has been done before with great success (i.e., look at what UCB did with ICSI). In our case, we simply have to take advantage of the EA transition vehicle and technology spinoff from GT that we have set up already; VLI.

VLI as you very well know is Angelos' and mine technology spinoff so we have to manage all possible COI with great caution. But I do not think this is a showstopper.

But again, at the end of the day, VLI MUST hold the bulk of data already (and inevitably the bulk of the risk) already because it has been set up to serve the operational needs of DoD when it comes to the EA technology. In my mind, it makes no sense to duplicate this risk in GT. So the million dollar question is the following: How can we keep the risk contained at VLI while enabling more research in GT?

Do we need a blanket COI about how people can work with VLI's data in GT? How can GT and VLI jointly bid on proposals as primes --- so we can keep paying the GRAs in GT and at the same time have experts in the field manage the risk and the operational aspects of the technology transition at VLI?

How can we create the proper dynamic between VLI and GT where GT remains the leading research unit in this space and GT clearly acknowledges VLI as the de facto transition vehicle for this research? How can the IP created in GT, by GT researchers yet with data that VLI holds can then be licensed by VLI or the inventor of the technology without throwing VLI's interest under the bus (from a technology and competition point of view)?

We are probably breaking new grounds here and I am not sure if and how any of these are even possible. That being said, I do think that this is a well worth problem spending some time thinking about.

I do not want to give up GT, I do not want to allow a politically motivated body of the DoJ to take away a research area from GT --- a research area that was created by people in this email thread. That is simply unAmerican. But, I cannot be blind and ignorant anymore about what happened the last two months and what will almost certainly happen again in the years to come as political tensions rise.

To that end I would like to set up a meeting as early as possible with all of you to discuss what is possible and what is not. If a mutually beneficial solution that reduces or at least significantly manages the risk for all parties involved can be identified, we should then loop in legal or anyone else necessary to start writing things down in a MoU.

Gentlemen, as I have said before, this is a research area Angelos and I created. We cannot simply walk away from it.

Thanks, Manos

From: "Nie, Ling-Ling" <linglingnie@gatech.edu>

Date: Saturday, July 24, 2021 at 11:32 AM

To: "Antonakakis, Manos" <manos@gatech.edu>, "McLaughlin, Steven W" <swm@gatech.edu>, "Abdallah, Chaouki T" <ctabdallah@gatech.edu>

Subject: Re: FGJ Subpoena for Manos Antonakakis

Hi Manos: Thank you for your thoughtful email. I know these last few weeks have been a whirlwind. I will ask my assistant to reach out on Monday to schedule time for all of us to talk further.

Ling-Ling

From: Antonakakis, Manos <manos@gatech.edu>

Sent: Saturday, July 24, 2021 10:50 AM

To: McLaughlin, Steven W; Abdallah, Chaouki T; Nie, Ling-Ling

Subject: Re: FGJ Subpoena for Manos Antonakakis

Hey Steve, Chaouki and Ling-Ling,

Hope you are doing great.

I have not been bothering you about this because I have been told by Christian (who is an absolute Rock star!) that Ling-Ling (or someone in her team) has been communicating to you what is going on with this situation.

This email is not about me explaining to you that I have done nothing wrong. I suspect that now that Christian has all the information he needs he can independently arrive at that conclusion and communicate what needs to be communicated to you.

This email is about the key question, "And now what?"

From where I stand, and for the first time in my life I felt that I am being investigated by law enforcement because of my ideas and the work I have done for the USG/DoD. For the first time since the moment I landed in Dulles international airport on October 1st of 2004, I had a serious discussion with my wife about moving back to Greece. Most importantly, however, I brought unnecessary attention from the DoJ in my working environment. This besides potentially hurting my reputation within GT (even if it is from an optics point of view) it also personally disappoints me greatly, because as a GT PhD student (2006-2012) and now as a faculty (2014-now) I always had as a goal to bring good news, recognition and success to GT --- and certainly not the attention of a special council.

If I make an attempt to come in your shoes, it would be absolutely reasonable for all of you to have questions about the risk that my research (and perhaps even myself) could bring to the Institute in the future. Therefore, when the dust settles I would like to have a discussion with all of you about the following two key open questions:

1. First and foremost, how do you feel about my actions now that GT legal has a plethora of my emails and after I spent countless hours explaining to everyone why I did what I did at the time I did it? If you think I did something unethical (not necessarily illegal) I will work with GT to smoothly (see running projects, students, SOW deliverables, etc.) or otherwise transition out. You have my word on this.
2. Big data analysis and machine learning for attack attribution is the future. After all these events with this politically driven inquisition, I need to see if there is a place where I can keep working on this research space that I invented over the last 5 years through my work in EA. What I would like to know is how GT upper management and legal feels about my line of research after all these events? Is GT a place that would welcome more innovation in this space, or this is simply not your (read is as GT's) cup of tea anymore?

Finally, I will leave you with an anecdote and a thought. During one of my interviews with the Special Counsel prosecutor, I was asked point blank by Mr. DeFilippis, "Do you believe that DARPA should be instructing you to investigate the origins of a hacker (Guccifer_2.0) that hacked a political entity (DNC)?" Let that sync for a moment, folks. Someone hacked a political party (DNC, in this case), in the

middle of an election year (2016), and the lead investigator of DoJ's special council would question whether US researchers working for DARPA should conduct investigations in this matter is "acceptable"! While I was tempted to say back to him "What if this hacker hacked GOP? Would you want me to investigate him then?", I kept my cool and I told him that this is a question for DARPA's director, and not for me to answer.

Steve, Chaouki and Ling-Ling; please, try to imagine a "United States of America" where investigations and prosecutions are determined by ideas and political beliefs. This has been tried before in human history and the results of it was forced labor and Gulags.

Folks, I strongly believe we will need this type of research and much more innovation in this space to preserve our democracy. This is factually true for a single yet fundamental reason: data driven scientific attribution is unbiased politically. Data belongs to no political party. Our nation's adversaries will keep attacking our country --- I am certain of this because their attacks simply work and are tremendously impactful to our society.

Thank you and have a great weekend.

PS. I am writing this email on a weekend because this is my first downtime since July 2nd when I received the subpoena.

Thanks, Manos

From: "Nie, Ling-Ling" <linglingnie@gatech.edu>

Date: Friday, July 2, 2021 at 7:50 PM

To: "Antonakakis, Manos" <manos@gatech.edu>, "McLaughlin, Steven W" <swm@gatech.edu>, "Abdallah, Chaouki T" <ctabdallah@gatech.edu>, "Wasch, Kate" <kate.wasch@legal.gatech.edu>, "Lunon, Darryl" <dl91@gatech.edu>

Subject: Re: FGJ Subpoena for Manos Antonakakis

Hi Manos: Thanks for forwarding. I'm copying Kate's correct email address and adding Darryl. We will confer internally and come back to you early next week as there are some people who are out of the office for the holiday weekend that we will need to loop in.

From: Antonakakis, Manos <manos@gatech.edu>

Sent: Friday, July 2, 2021 2:39 PM

To: McLaughlin, Steven W; Abdallah, Chaouki T; kate.wesch@legal.gatech.edu; Nie, Ling-Ling

Subject: Fw: FGJ Subpoena for Manos Antonakakis

Hey Steve/Chaouki/Kate/Ling-Ling,

Hope you are doing great! Evidently I need to appear in front of a Grand Jury on July 15th. Any idea if I should talk with GT counsel before or if anyone from GT should be with me in this testimony?

This is a first for me so I am not sure what to do next.

Thanks, Manos

From: Eckenrode, John (JMD) <John.Eckenrode@usdoj.gov>

Sent: Friday, July 2, 2021 4:28 PM

To: Antonakakis, Manos

Cc: kate.wesch@legal.gatech.edu; Fuhrman, Tim (JMD)

Subject: FGJ Subpoena for Manos Antonakakis

Dear Mr. Antonakakis - This is Jack Eckenrode, an Investigator with the US Justice Department. Together with my colleague Tim Fuhrman, copied here, with whom you may have had previous contact, we are attaching a federal grand jury subpoena seeking your testimony in Washington, DC on July 15, 2021 at 1:00pm. You should feel free to contact either one of us in the event that you have any questions related to the subpoena or your appearance.

Also copied for her awareness is Kate Wasch, legal counsel from Georgia Tech.

Exhibit 4

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

....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.

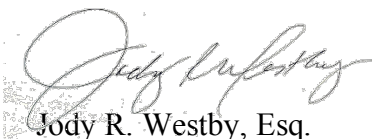
We are happy to address any concerns that you may have in this regard, but it seems clear to us that a person employed as a security researcher who conducts security research for his employer, and also brings millions of dollars in research grants to the school from this research, is acting within the 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