

EXHIBIT B



BOSTON CONNECTICUT NEW JERSEY NEW YORK WASHINGTON, DC

STANLEY A. TWARDY, JR.
Attorney at Law

One Canterbury Green
Stamford, CT 06901-2047
T: (203) 977-7368 F: (866) 458-1037
satwardy@daypitney.com

October 19, 2015

VIA UPS

The Honorable Ron Johnson
Chairman
Committee on Homeland Security & Governmental Affairs
United States Senate
Washington, D.C., 20510

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security & Governmental Affairs
United States Senate
Washington, D.C., 20510

Dear Chairman Johnson and Ranking Member Carper:

We represent Datto, Inc., (“Datto”) and write further to our October 7, 2015 letter in response to Chairman Johnson’s letter to Datto Chief Executive Officer Mr. Austin McChord dated October 5, 2015.

In your October 5th letter, you requested that Datto voluntarily provide certain information to assist the Committee to “better understand Datto’s role relating to Secretary Clinton’s private server, the backup and security capabilities of the private server, and any directives provided to Datto relating to the server.”¹ This letter responds to those requests and reiterates Datto’s intention to continue responding to and complying with the requests in your letter, to the extent permitted by Datto’s data privacy policies and its contractual confidentiality requirements.

¹ Letter from The Honorable Ron Johnson to Mr. Austin McChord, dated October 5, 2015, at p. 4. It is our understanding that your request contemplates a voluntary response, and that no subpoena has issued pursuant to the *Rules of Procedure of the Committee on Homeland Security and Governmental Affairs*, March 2015.

The Honorable Ron Johnson
The Honorable Thomas R. Carper
October 19, 2015
Page 2

The relevant terms of those requirements as stated in a typical Reseller Agreement include:

“Confidential Information” means any information, whether oral, written, electronic, or in any other format, and whether technical or business in nature, regarding this Agreement, Datto’s products or business, including the Product, information regarding a party’s products, services, Marks, software, intellectual property, equipment, pricing, marketing and business plans, other information not generally known to the public and any other information received under circumstances reasonably interpreted as imposing an obligation of confidentiality; provided that, “Confidential Information” shall not include any of such information which: (i) was publicly available at the time of disclosure by the disclosing party; (ii) became publicly available after disclosure through no fault of the receiving party; (iii) was known to the receiving party prior to disclosure by the disclosing party; or (iv) was rightfully acquired by the receiving party after disclosure by the disclosing party from a third party who was lawfully in possession of the information and was under no legal duty to the disclosing party to maintain the confidentiality of the information.

Required Disclosures. Either party may disclose Confidential Information to the extent disclosure is based on the good faith written opinion of such party’s legal counsel that disclosure is required by law or by order of a court or governmental agency; provided that, the party that is the recipient of such Confidential Information shall use all commercially reasonable efforts to maintain the confidentiality of the Confidential Information by means of a protective order or other similar protection and shall give the owner of such Confidential Information prompt notice in order that it have every opportunity to intercede in such process to contest such disclosure and shall use all commercially reasonable efforts to cooperate with the owner of such Confidential Information to protect the confidentiality of such Confidential Information. The owner of such Confidential Information reserves the right to obtain a protective order or otherwise protect the confidentiality of such Confidential Information.

On October 6, 2015, in accordance with its obligations under the Reseller Agreement, Datto notified Platte River Networks (“Platte River”) of your October 5 inquiry, and asked whether they would object to disclosure of the information and materials requested. Platte River advised us that they had “no objection.” However, on October 14, 2015, counsel to Platte River withdrew their previous non-objection, and objected to any further disclosure of Confidential Information (as defined in the Reseller Agreement) to the Committee. Accordingly, Datto cannot disclose any such Confidential Information unless required by law or by order of a court or governmental agency.

The Honorable Ron Johnson
The Honorable Thomas R. Carper
October 19, 2015
Page 3

Our review of documents and other materials related to your requests continue, and should that effort reveal additional information responsive to your requests that is not confidential, we will supplement this response.

I. BACKGROUND

Datto is a back-end service provider to thousands of managed IT service providers – often referred to as Managed Service Providers (“MSPs”) or “Resellers” such as Platte River. MSPs are often sophisticated, professional companies that provide a defined set of IT operations and services to their clients or “End-Users.” Datto works almost exclusively with these MSPs to provide comprehensive and secure “hybrid cloud” backup, data recovery, and business continuity solutions that the MSPs in turn resell and administer to End-Users. To accomplish this, Datto provides hardware, software and technical services to MSPs, as more fully described below. Datto also provides MSP customers with training on how to use Datto services.

Datto’s services to MSPs are generally governed by Reseller Agreements between the MSP and Datto. These contracts contain mutual and binding confidentiality clauses. As previously discussed, such a clause applies in Datto’s contract with Platte River. Rarely does Datto deal directly with an End-User, and in the matter referred to in your inquiry, Datto’s contractual relationship was with Platte River only. Datto was not aware of the identity of the End-User until reading allegations in the media.

Datto’s hybrid cloud solution involves two parts: (i) a local hardware backup device, such as the Datto SIRIS device (a “Local Device”); and (ii) a replicated offsite backup.² First, the Datto solution uses software to take a full backup image of the End-User’s IT environment that is being backed up (servers, data, etc.) and copies it onto a Local Device, which is a hardware device that is often located in the same physical location as the IT environment it is backing up (i.e. the “server room”). From there, the Local Device works as a “failover” system in the event of a business interruption that impacts the End-User’s IT environment. Second, a duplicate copy of all of the information stored on the Local Device is also placed on a replicated storage device (a “Storage Node”) that is located at a different location (i.e. “offsite”) than the Local Device.³ Offsite replication ensures that if the event that caused the End-User’s system to fail also impacts the Local Device (e.g. a fire or flood) the MSP can use the cloud – “Datto Cloud” or a “Private Cloud” – as an alternative failover system from the Local Device.

In most use cases, the MSP chooses for offsite replication to occur at a Datto-controlled data center facility. Datto refers to this approach as a “Datto Cloud” solution. In other use cases,

² In this letter “local” refers to the physical location of the MSP’s systems.

³ This duplication is accomplished by the creation of multiple restore points that can be individually reconstructed to restore the dataset as it previously existed at a particular time.

The Honorable Ron Johnson
The Honorable Thomas R. Carper
October 19, 2015
Page 4

MSPs may choose to replicate backed-up data offsite to a Storage Node owned and operated by the MSP at a site of its choosing. Datto refers to this approach as a “Private Cloud.”

As an alternative to a hybrid cloud approach, an MSP may opt out of offsite replication altogether and request a “Local Only” setup. In a Local Only configuration, backed-up data will not replicate beyond the Local Device. Because Datto’s technology solution is meant to be deployed as a hybrid cloud solution, to set up a Local Only solution, generally the MSP must work directly with Datto technical support to implement this. By default, absent a functioning private offsite Storage Node or the requisite communications with Datto technical support, all Local Devices replicate to the Datto Cloud.

As noted, as a back-end service provider, Datto very rarely—if ever—has any direct interaction with the End-Users served by the MSPs. The nature of Datto’s relationship with MSPs precludes Datto from knowing either the identity of End-Users and the content of the data stored on the Local Device or replicated offsite. Datto has no role in monitoring the content or source of data stored by MSP clients such as Platte River. As such, Datto would not be aware of who was Platte River’s End-User and Datto did not and does not have any knowledge concerning the content of any data that may or may not have been backed up to the Datto Cloud, or stored on the Datto SIRIS device owned and operated by Platte River.⁴

II. DATTO INVOLVEMENT IN MATTERS RELATED TO THE COMMITTEE’S INQUIRY

Datto first became aware that Platte River had been contacted by U.S. Government officials inquiring into Platte River’s involvement with former Secretary Clinton’s e-mail server through media reports on or about Sunday, August 9, 2015. Soon thereafter, Datto disconnected the replicated offsite Storage Node, and independently took prudential steps to preserve information within Datto’s control which Datto believed could be subject to law enforcement or other governmental inquiry.

On September 10, 2015, Datto received a *Request for Preservation of Records* from the Federal Bureau of Investigation (FBI) requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. The FBI has custody of the Storage Node.

⁴ Datto’s standard contracts permit communication with an End-User, but this rarely is done, and was not in this case. In rare cases, Datto will be asked to directly assist an End-User.

The Honorable Ron Johnson
The Honorable Thomas R. Carper
October 19, 2015
Page 5

III. RESPONSES TO INFORMATION REQUESTS

Please note that with respect to questions 1-4, 7, 8 and 9, these requests call for the production of documents and materials that are Confidential Information as defined by the Datto Reseller Agreement and Datto's data privacy policies. Consequently, Datto is not authorized to disclose such information absent consent from its client, Platte River, or unless required by law or by order of court or governmental agency.

With respect to questions to which the immediately preceding paragraph does not apply, Datto responds as follows:

5. *Is Datto authorized to store classified information? Were any Datto employees authorized to view classified information? Please explain. Did Datto's contract regarding Secretary Clinton's private server include provisions related to the storing of classified information?*

RESPONSE: Datto is not authorized to store classified information, and does not offer storage of classified information as part of its business.⁵ No Datto employees are authorized to access classified information in the context of their employment at Datto. Datto has never entered into any contracts containing provisions related to the storage of classified information.

6. *Has Datto been contacted by the Federal Bureau of Investigation (FBI) or any other law-enforcement entity regard (sic) Secretary Clinton's private server? Has Datto turned over any information, materials, or equipment to the FBI or any other law enforcement entity? Please explain.*

RESPONSE: On September 10, 2015, Datto received a *Request for Preservation of Records* from the FBI, requesting that Datto preserve records related to a Datto Local Device identified by the FBI. Datto informed the FBI on September 16, 2015 that Datto had disconnected and preserved an offsite Storage Node associated with the Local Device. On October 6, 2015, with the consent of Platte River and its End-User, Datto provided the Storage Node to the FBI. The FBI has custody of the Storage Node.

8. *Please explain the process for storing data in the Datto Cloud.*
a. *How long is data retained in the cloud?*
b. *What happens to the data once the required retention period is reached?*

⁵ For purposes of this response "classified information" means information classified pursuant to Executive Order 13526. Datto does not hold a Facilities Clearance (FCL) as administered by the Defense Security Service, or any other U.S. Government agency or department.

The Honorable Ron Johnson
The Honorable Thomas R. Carper
October 19, 2015
Page 6

- c. *Is the data deleted automatically?*
- d. *As mentioned above, CESC requested that the retention period for backups be reduced to 30 days. What information would be lost by reducing the backup retention period to 30 days? Please explain.*

RESPONSE: To the extent Chairman Johnson's request calls for a general outline of the process for storing data in the Datto Cloud, or Datto's security capabilities and functions, we note that Datto's security efforts include hardware, software, and encryption mechanisms as well as physical, technical and administrative controls. The details of these capabilities are confidential, and public disclosure of those details could reveal vulnerabilities and capabilities of Datto's systems, infrastructures, projects, plans, or protection services relating to its business and the data entrusted to Datto by its MSP customers. As such, public disclosure of these capabilities could cause Datto's systems to become less secure.

The Datto Cloud has over 140 petabytes of cloud storage capacity. Usage of that storage capacity fluctuates depending on the retention settings established by the MSP. That said, Datto's solution takes an exact and comprehensive backup image of the entire host machine that it backs up. The Datto solution will keep an image of everything that was on the host machine when the last backup was taken. Users generally take that image every day, usually more than once per day. The data is stored in a snapshot capable file system that tracks the state of the backups back in time. At any one point, the solution will have the most recent copy of the machine it backs up as well as a number of exact copies of prior versions depending on the retention settings that the MSP has chosen. If the retention settings are 30 days, that means that the picture the Datto Solution takes on day 1 will roll off the backup chain on day 31.

The following is an example of how a specific retention setting would apply to a theoretical unit of data. This example assumes a 30 day retention setting, and that user settings provide for only one full backup per day.

Day 1 – The backup includes a word document (“Document A”) that is sitting on the host machine.

Day 15 – Before the day's backup was taken, the user makes changes to Document A. Rather than saving the changes to a new word document, the user just writes over Document A.

Day 30 – The user realizes that she liked the way Document A was drafted before she wrote over it. The Datto solution took an image of Document A on each of days 1 through 14 (before it was written over). The user can retrieve that Document A from the backup images made on days 1 through 14.

The Honorable Ron Johnson
The Honorable Thomas R. Carper
October 19, 2015
Page 7

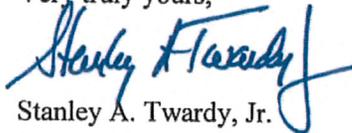
Day 60 -- Assume that the user did not realize until day 60 that she liked the way Document A was drafted before she changed it. Document A is no longer recoverable because the last backup of that document would have dropped off the backup chain on day 44.

That said, an image based backup is a sparse file. It is a block by block copy of the host machine that it backs up. When data is removed from the file system, in most cases the file system does not automatically "zero out" the de-referenced blocks on a hard drive. Rather, a metadata store marks those blocks as free for future use. So, there remains a potential that de-referenced blocks of data may still reside on a hard drive.

IV. CONCLUSION

Thank you for the opportunity to assist the Committee in its work. Please do not hesitate to contact me if you have any questions.

Very truly yours,



Stanley A. Twardy, Jr.

cc: Michael Joseph Lueptow
Investigative Counsel
Committee on Homeland Security & Governmental Affairs
United States Senate
Washington, D.C., 20510
Via E-mail

Scott D. Wittmann
Investigative Counsel
Committee on Homeland Security & Governmental Affairs
United States Senate
Washington, D.C., 20510
Via E-mail

James Secreto
Chief Counsel for Oversight and Investigations (Minority)
Committee on Homeland Security & Governmental Affairs
United States Senate
Washington, D.C., 20510
Via E-mail