UNITED STATES DISTRICT COURT
IN THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

DATA SCAPE LIMITED,

Plaintiff,

v.

DROPBOX, INC.,

Defendant.

C.A. No. 6:19-cv-00023

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq.* in which plaintiff Data Scape Limited ("Plaintiff," "Data Scape") makes the following allegations against defendant Dropbox, Inc. ("Defendant," "Dropbox"):

PARTIES

1. Data Scape is a company organized under the laws of Ireland with its office located at Office 115, 4-5 Burton Hall Road, Sandyford, Dublin 18, Ireland.

2. On information and belief, Defendant Dropbox, Inc. is a Delaware corporation with a principal place of business at 333 Brannan Street, San Francisco, CA 94107. Dropbox may be served through its registered agent, Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

JURISDICTION AND VENUE

3. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

4. This Court has personal jurisdiction over the defendant in this action because the defendant has committed acts within the Western District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over the defendant would not offend traditional notions of fair play and substantial justice. The defendant, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the asserted patents.

5. Venue is proper in this district under 28 U.S.C. § 1400(b). Upon information and belief, Dropbox is registered to do business in Texas. Upon information and belief, Dropbox has transacted business in the Western District of Texas and has committed acts of direct and indirect infringement in this District. Dropbox has a regular and established place of business in Western District of Texas. For example, Dropbox an office in Austin, Texas where it employs sales and user operations teams.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 7,720,929

6. Data Scape is the owner by assignment of United States Patent No. 7,720,929 ("the '929 Patent"), entitled "Communication System And Its Method and Communication Apparatus And Its Method." The '929 Patent was duly and legally issued by the United States Patent and Trademark Office on May 18, 2010. A true and correct copy of the '929 Patent is included as Exhibit A.

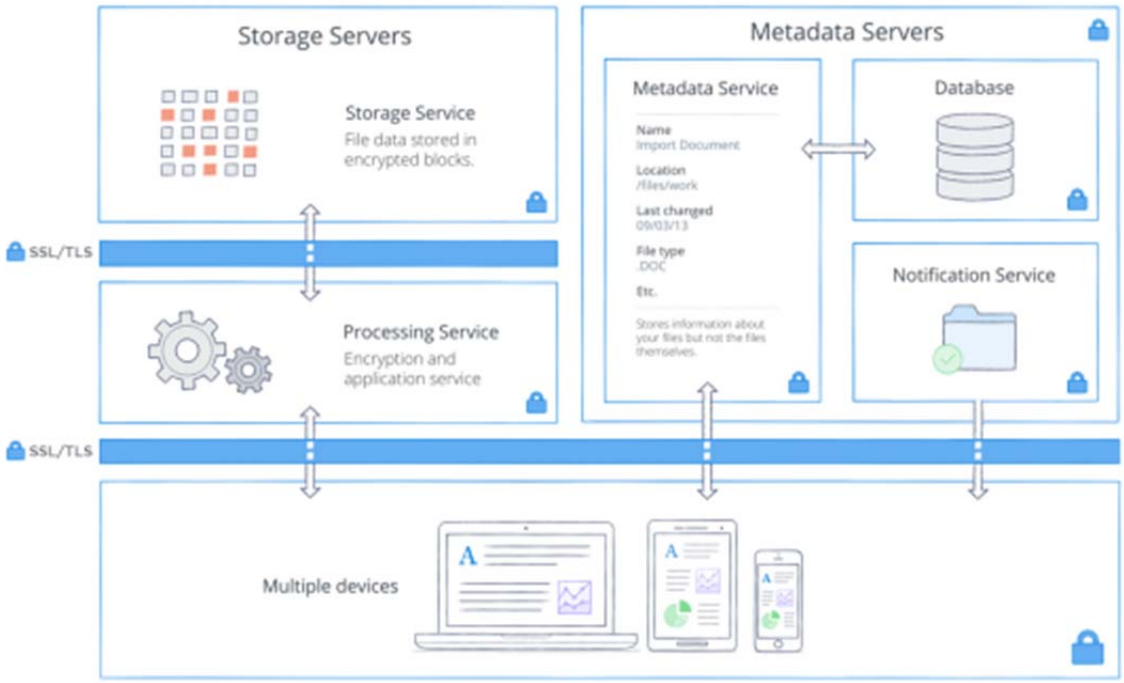
7. Dropbox has offered for sale, sold and/or imported into the United States products and services that infringe the '929 patent, and continues to do so. By way of

illustrative example, these infringing products and services include, without limitation, Defendant's products and services, *e.g.*, Dropbox services, including Dropbox Business, and all versions and variations thereof since the issuance of the '929 Patent ("Accused Instrumentalities").

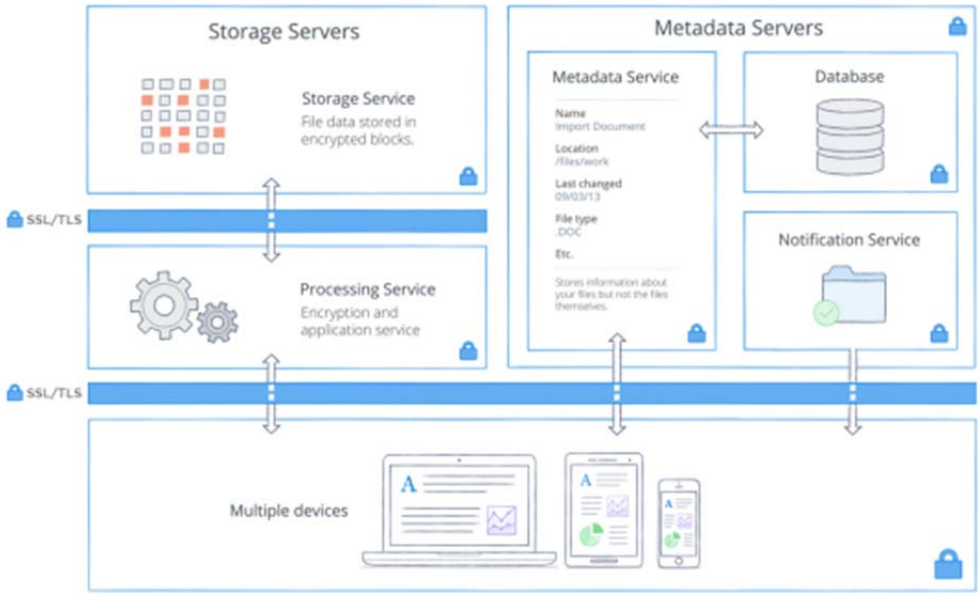
8. Dropbox has directly infringed and continues to infringe the '929 Patent, for example, by making, selling, offering for sale, and/or importing the Accused Instrumentalities, and through its own use and testing of the Accused Instrumentalities. Dropbox uses the Accused Instrumentalities for its own internal non-testing business purposes, while testing the Accused Instrumentalities, and while providing technical support and repair services for the Accused Instrumentalities to its customers.

9. For example, the Accused Instrumentalities infringe Claim 1 (as well as other claims) of the '929 Patent. One non-limiting example of the Accused Instrumentalities' infringement is presented below:

10. The Accused Instrumentalities include "[a] communication system including a first apparatus having a first storage medium, and a second apparatus." For example, Dropbox Business communicates data stored on a second apparatus (e.g. Dropbox servers and associated services) to a first apparatus with a first storage medium (e.g. a user's device with the Dropbox desktop app installed). *See, e.g.*, "Dropbox Business Security" *available at* https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf:



11. The Accused Instrumentalities include a second apparatus comprising: "a second storage medium configured to store management information of data to be transferred to said first storage medium." For example, Dropbox Business includes a storage medium (e.g., the various servers and associated services) configured to store management information (e.g., metadata and sync settings for Smart Sync) of data to be transferred to the user device. *See, e.g.*, "Dropbox Business Security" at 4-5:



Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the **Encryption** section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

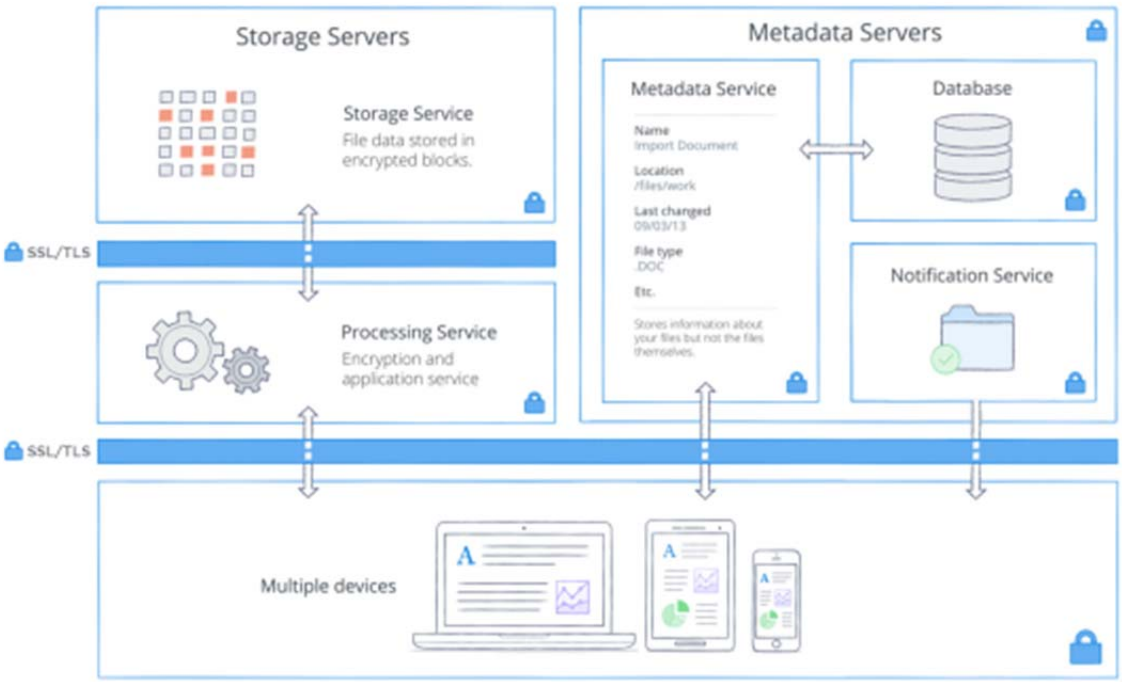
File data storage

Dropbox stores metadata about files (such as the date and time a file was last changed) and the actual contents of files (file blocks). File metadata is stored on Dropbox servers. File content is stored in one of two systems: Amazon Web Services (AWS) or Magic Pocket, Dropbox's in-house storage system. Magic Pocket consists of both proprietary software and hardware and has been designed from the ground up to be reliable and secure. In both Magic Pocket and AWS, file blocks are encrypted at rest, and both systems meet high standards for reliability. For more details, please see the **Reliability** section below.

See also "Smart Sync" available at https://www.dropbox.com/help/desktop-web/smart-sync:

> Smart Sync is a Dropbox feature that helps you save space on your hard drive. Access every file and folder in your Dropbox account from your computer, using virtually no hard drive space. Smart Sync is available for Dropbox Professional customers, and members of Dropbox Business teams. With Smart Sync, you can:
>
> - Choose if individual files or folders are available online-only or locally on your computer
> - Select a default sync setting for new files and folders that are shared with you

12. The Accused Instrumentalities further include a second apparatus comprising "a communicator configured to communicate with said first apparatus." For example, Dropbox Business provides a communicator (e.g., one that uses SSL/TLS protocols) configured to communicate with the first apparatus (e.g. a user device). *See, e.g.*, "Dropbox Business Security" at 4, 5:



Sync

Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

- **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
- **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
- **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

13. The Accused Instrumentalities further include a second apparatus comprising "a detector configured to detect whether said first apparatus and a second apparatus are connected." For example, Dropbox Business includes a detector configured to determine when the user device is connected (e.g. linked devices). *See, e.g.*, "Dropbox Business Security" at 3-5:

Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

Sync

Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

- **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
- **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
- **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

14. The Accused Instrumentalities further include a second apparatus comprising "an editor configured to select certain data to be transferred and to edit said management information based on said selection without regard to the connection of said first apparatus." For example, Dropbox Business includes an editor configured to select

certain data to be transferred and to edit the management information (e.g. metadata and sync settings for Smart Sync) based on the selection without regard to the connection of the user device. *See, e.g.*, "Smart Sync for Team Admins" *available at* https://www.dropbox.com/help/desktop-web/smart-sync-admins:

> Smart Sync helps you and your team share content without worrying about overloading your hard drives. Smart Sync team settings are available to Dropbox Business team admins.
>
> When your team starts using Smart Sync, content that's already downloaded to team member devices remains downloaded. New content is automatically online-only unless you change this setting in the Admin Console. Team members can also chose a personal default for each of their connected computers.
>
> The Smart Sync default applies to new content after the default is enabled and isn't retroactive. The Smart Sync default applies to:
>
> - Joining a shared folder
> - Linking a new device
> - Adding new content from another computer
>
> To set a default for your team:
>
> 1. Sign in to dropbox.com with your admin account.
> 2. Click **Admin Console**.
> 3. Click **Settings**.
> 4. Click **Smart Sync**.
> 5. Select a default for Smart Sync:
>
>   - Synced locally
>   - Online-only

See also "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:

> Smart Sync is a Dropbox feature that helps you save space on your hard drive. Access every file and folder in your Dropbox account from your computer, using virtually no hard drive space. Smart Sync is available for Dropbox Professional customers, and members of Dropbox Business teams. With Smart Sync, you can:
>
> - Choose if individual files or folders are available online-only or locally on your computer
> - Select a default sync setting for new files and folders that are shared with you

15. The Accused Instrumentalities further include a second apparatus comprising "a controller configured to control transfer of the selected data stored in said second apparatus to said first apparatus via said communicator based on said management information edited by said editor when said detector detects that said first apparatus and said second apparatus are connected." For example, Dropbox Business includes a controller configured to control transfer of the selected data stored in the Storage Servers to the user device when the user device is connected. *See, e.g.*, "Dropbox Business Security" at 3-5:

> Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

See also "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:

With Smart Sync, content on your computer is available as either online-only, local, or in mixed state folders.

Online-only content

Online-only content appears in the Dropbox folder on your computer, but doesn't use the full amount of space that the file otherwise would. You can see the file, but the content isn't fully downloaded until you need it. Only information about the file, such as the file name, location, and date the file was updated, is downloaded.

Local content

Local content is downloaded and saved on the hard drive of your computer. You can directly edit these files from applications on your computer. This content is still backed up to Dropbox as well.

Mixed state folders

Mixed state folders contain both local and online-only content.

16. The Accused Instrumentalities further include a second apparatus wherein said controller is configured to compare said management information edited by said editor with management information of data stored in said first storage medium and to transmit data in said second apparatus based on result of the comparison." For example, Dropbox Business includes a controller configured to compare the management information edited by the editor with management information of data stored in the user device (e.g. through the Processing Service, the Metadata Service, or the Notification

Service), and transmits data in the various servers of Dropbox Business based on the result of the comparison. *See, e.g.*, "Dropbox Business Security" at 3-5:

Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

Sync

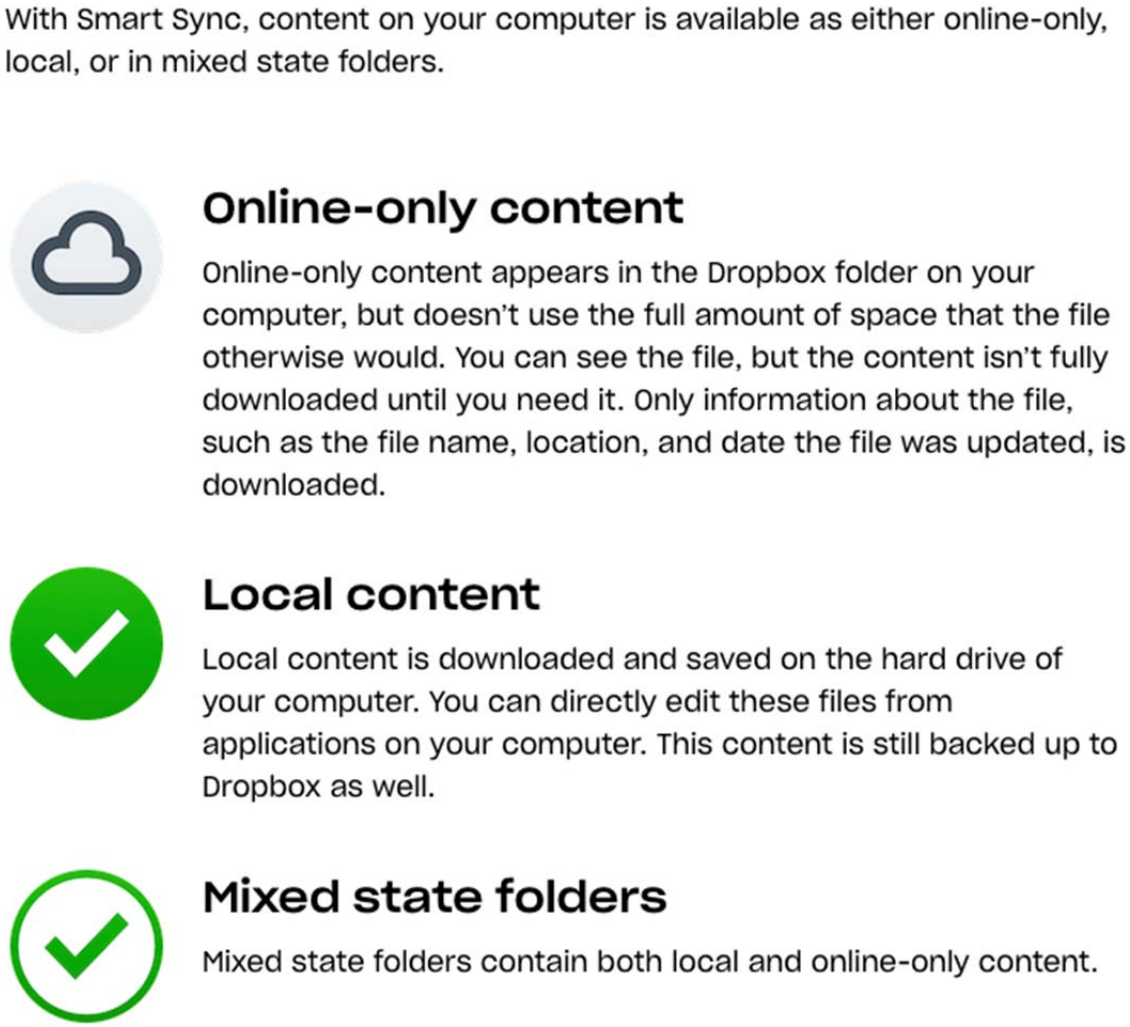
Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

- **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
- **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
- **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

See also "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:



17. Dropbox has had knowledge of the '929 Patent and its infringement since at least the filing of the original Complaint in this action, or shortly thereafter, including by way of this lawsuit. By the time of trial, Dropbox will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of the claims of the '929 Patent.

18. Dropbox's affirmative acts of making, using, selling, offering for sale, and/or importing the Accused Instrumentalities have induced and continue to induce users of the Accused Instrumentalities to use the Accused Instrumentalities in their

normal and customary way to infringe the claims of the ’929 Patent. Use of the Accused Instrumentalities in their ordinary and customary fashion results in infringement of the claims of the ’929 Patent.

19. For example, Dropbox explains to customers the benefits of using the Accused Instrumentalities, such as by touting their advantages of saving space on hard drives and maintaining access to stored files without using hard drive space in the case of the Dropbox Business feature named “Smart Sync.”. Dropbox also induces its customers to use the Accused Instrumentalities to infringe other claims of the ’929 Patent. Dropbox specifically intended and was aware that the normal and customary use of the Accused Instrumentalities on compatible systems would infringe the ’929 Patent. Dropbox performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ’929 Patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Dropbox engaged in such inducement to promote the sales of the Accused Instrumentalities, *e.g.*, through its user manuals, product support, marketing materials, demonstrations, installation support, and training materials to actively induce the users of the accused products to infringe the ’929 Patent. Accordingly, Dropbox has induced and continues to induce end users of the accused products to use the accused products in their ordinary and customary way with compatible systems to make and/or use systems infringing the ’929 Patent, knowing that such use of the Accused Instrumentalities with compatible systems will result in infringement of the ’929 Patent. Accordingly, Dropbox has been (since at least as of filing of the original complaint), and currently is, inducing infringement of the ’929 Patent, in violation of 35 U.S.C. § 271(b).

20. Dropbox has also infringed, and continues to infringe, claims of the ’929 Patent by offering to commercially distribute, commercially distributing, making, and/or importing the Accused Instrumentalities, which are used in practicing the process, or using the systems, of the ’929 Patent, and constitute a material part of the invention. Defendant knows the components in the Accused Instrumentalities to be especially made or especially adapted for use in infringement of the ’929 Patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. For example, the ordinary way of using the Accused Instrumentalities infringes the patent claims, and as such, is especially adapted for use in infringement. Accordingly, Dropbox has been, and currently is, contributorily infringing the ’929 Patent, in violation of 35 U.S.C. § 271(c).

21. For similar reasons, Dropbox also infringes the ’929 Patent by supplying or causing to be supplied in or from the United States all or a substantial portion of the components of the Accused Instrumentalities, where such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the ’929 Patent if such combination occurred within the United States. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., storage and metadata servers) and software (e.g., Dropbox Business software) components of the Accused Instrumentalities in such a manner as to actively induce the combination of such components (e.g., by instructing users to rely on multiple servers that save redundant copies of metadata and content in a typical Dropbox Business system) outside of the United States.

22. Dropbox also indirectly infringes the ’929 Patent by supplying or causing to be supplied in or from the United States components of the Accused Instrumentalities that are especially made or especially adapted for use in infringing the ’929 Patent and are not a staple article or commodity of commerce suitable for substantial non-infringing use, and where such components are uncombined in whole or in part, knowing that such components are so made or adapted and intending that such components are combined outside of the United States in a manner that would infringe the ’929 Patent if such combination occurred within the United States. Because the Accused Instrumentalities are designed to operate as the claimed system and apparatus, the Accused Instrumentalities have no substantial non-infringing uses, and any other uses would be unusual, far-fetched, illusory, impractical, occasional, aberrant, or experimental. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., separate Storage servers and Metadata servers) and software (e.g., Dropbox Business software) components that are especially made or especially adapted for use in the Accused Instrumentalities, where such hardware and software components are not staple articles or commodities of commerce suitable for substantial noninfringing use, knowing that such components are so made or adapted and intending that such components are combined outside of the United States, as evidenced by Dropbox’s own actions or instructions to users, and enabling and configuring the infringing functionalities of the Accused Instrumentalities.

23. As a result of Defendant’s infringement of the ’929 Patent, Plaintiff Data Scape is entitled to monetary damages in an amount adequate to compensate for

Dropbox's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dropbox, together with interest and costs as fixed by the Court.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 7,617,537

24. Plaintiff realleges and incorporates by reference the foregoing paragraphs, as if fully set forth herein.

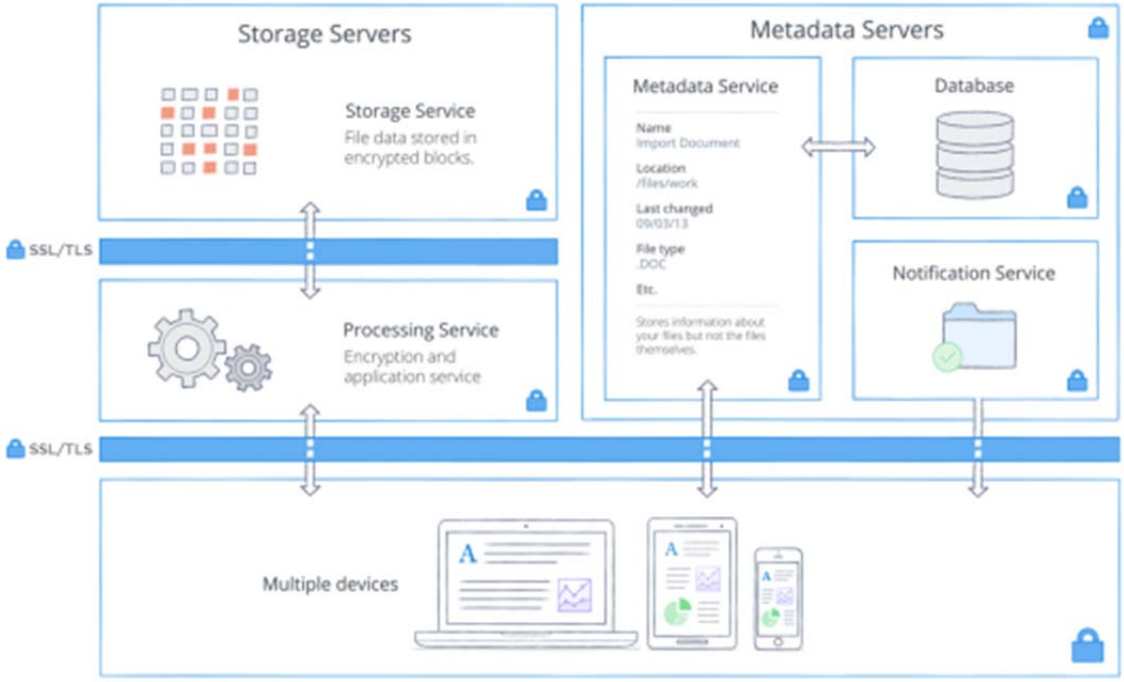
25. Data Scape is the owner by assignment of United States Patent No. 7,617,537 ("the '537 Patent"), entitled "Communication System And Its Method and Communication Apparatus And Its Method." The '537 Patent was duly and legally issued by the United States Patent and Trademark Office on November 10, 2009. A true and correct copy of the '537 Patent is included as Exhibit B.

26. Dropbox has offered for sale, sold and/or imported into the United States products and services that infringe the '537 patent, and continues to do so. By way of illustrative example, these infringing products and services include, without limitation, Defendant's products and services, *e.g.*, Dropbox services, including Dropbox Business, and all versions and variations thereof since the issuance of the '537 Patent ("Accused Instrumentalities").

27. Dropbox has directly infringed and continues to infringe the '537 Patent, for example, by making, selling, offering for sale, and/or importing the Accused Instrumentalities, and through its own use and testing of the Accused Instrumentalities. Dropbox uses the Accused Instrumentalities for its own internal non-testing business purposes, while testing the Accused Instrumentalities, and while providing technical support and repair services for the Accused Instrumentalities to its customers.

28. For example, the Accused Instrumentalities infringe Claim 1 (as well as other claims) of the ’537 Patent. One non-limiting example of the Accused Instrumentalities’ infringement is presented below:

29. The Accused Instrumentalities perform a communication method to transfer content data from a first apparatus to a second apparatus. For example, the Accused Instrumentalities communicate and transfer a file or folder stored on one device (e.g. a Dropbox storage server) to another device(e.g. a user device with the Dropbox desktop app installed). *See, e.g.*, “Dropbox Business Security” *available at* https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf:



30. The Accused Instrumentalities perform a communication method to transfer content data from a first apparatus to a second apparatus further comprising “judging whether said first apparatus and said second apparatus are connected.” For

example, Dropbox Business will update only linked devices when files are added, changed, or deleted. *See, e.g.*, "Dropbox Business Security" at 3-5:

> Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.
>
> **Sync**
>
> Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.
>
> - **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
> - **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
> - **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

31. The Accused Instrumentalities perform a communication method to transfer content data from a first apparatus to a second apparatus further comprising "comparing, upon judging that said first apparatus and said second apparatus are connected, an identifier of said first apparatus with an identifier stored in said second apparatus." For example, Dropbox Business provides for different Smart Sync settings on different devices, which means different devices differentiate themselves with the Dropbox System through identifiers. *See, e.g.*, "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:

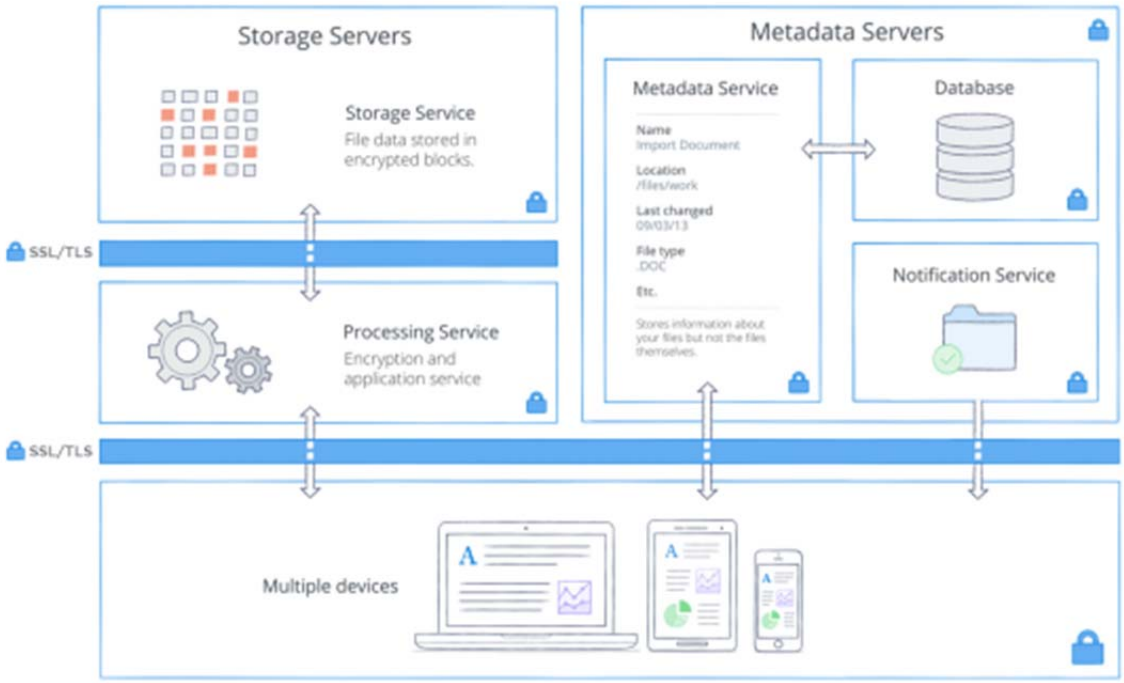
Smart Sync is a Dropbox feature that helps you save space on your hard drive. Access every file and folder in your Dropbox account from your computer, using virtually no hard drive space. Smart Sync is available for Dropbox Professional customers, and members of Dropbox Business teams. With Smart Sync, you can:

- Choose if individual files or folders are available online-only or locally on your computer
- Select a default sync setting for new files and folders that are shared with you

Can I have different Smart Sync settings on different devices?

Yes, Smart Sync settings are unique to each device you link to your Dropbox account.

32. The Accused Instrumentalities perform a communication method to transfer content data from a first apparatus to a second apparatus further comprising "comparing, when said identifier of said first apparatus corresponds to said identifier stored in second apparatus, a first list of content data of said first apparatus and a second list of content data of said second apparatus." For example, Dropbox Business provides for metadata services that act as an index for the data in users' accounts and synchronizes changes between files stored in a Storage Server and files on a linked device. *See, e.g.*, "Dropbox Business Security" at 3-5:



Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

33. The Accused Instrumentalities perform a communication method to transfer content data from a first apparatus to a second apparatus further comprising transferring, from the second apparatus to the first apparatus, first content data, which is registered in said second list and is not registered in said first list. For example, Dropbox

Business, upon determining that a linked device does not have a newly added or modified file, will update the linked device with the newly added or modified file. *See*, *e.g.*, "Dropbox Business Security" at 3-5:

> Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.
>
> Our architecture is comprised of the following services:
>
> - **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
> - **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
> - **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
> - **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.
>
> **Sync**
>
> Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.
>
> - **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
> - **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
> - **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

34. The Accused Instrumentalities perform a communication method to transfer content data from a first apparatus to a second apparatus further comprising deleting, from the first apparatus, second content data, which registered in said first list

and is not registered in the second list. For example, Dropbox Business, upon determining that a linked device contains a file that was deleted in a recent synchronization, will update the linked device by deleting the file from the linked device as well. *See, e.g.*, "Dropbox Business Security" at 3:

> Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

35. Dropbox has had knowledge of the '537 Patent and its infringement since at least the filing of the original Complaint in this action, or shortly thereafter, including by way of this lawsuit. By the time of trial, Dropbox will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of the claims of the '537 Patent.

36. Dropbox's affirmative acts of making, using, selling, offering for sale, and/or importing the Accused Instrumentalities have induced and continue to induce users of the Accused Instrumentalities to use the Accused Instrumentalities in their normal and customary way to infringe the claims of the '537 Patent. Use of the Accused Instrumentalities in their ordinary and customary fashion results in infringement of the claims of the '537 Patent.

37. For example, Dropbox explains to customers the benefits of using the Accused Instrumentalities, such as by touting their advantages of replicating data among multiple devices. Dropbox also induces its customers to use the Accused Instrumentalities to infringe other claims of the '537 Patent. Dropbox specifically intended and was aware that the normal and customary use of the Accused Instrumentalities on compatible systems would infringe the '537 Patent. Dropbox performed the acts that constitute induced infringement, and would induce actual

infringement, with the knowledge of the ’537 Patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Dropbox engaged in such inducement to promote the sales of the Accused Instrumentalities, *e.g.*, through its user manuals, product support, marketing materials, demonstrations, installation support, and training materials to actively induce the users of the accused products to infringe the ’537 Patent. Accordingly, Dropbox has induced and continues to induce end users of the accused products to use the accused products in their ordinary and customary way with compatible systems to make and/or use systems infringing the ’537 Patent, knowing that such use of the Accused Instrumentalities with compatible systems will result in infringement of the ’537 Patent. Accordingly, Dropbox has been (since at least as of filing of the original complaint), and currently is, inducing infringement of the ’537 Patent, in violation of 35 U.S.C. § 271(b).

38. Dropbox has also infringed, and continues to infringe, claims of the ’537 Patent by offering to commercially distribute, commercially distributing, making, and/or importing the Accused Instrumentalities, which are used in practicing the process, or using the systems, of the ’537 Patent, and constitute a material part of the invention. Defendant knows the components in the Accused Instrumentalities to be especially made or especially adapted for use in infringement of the ’537 Patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. For example, the ordinary way of using the Accused Instrumentalities infringes the patent claims, and as such, is especially adapted for use in infringement. Accordingly, Dropbox has been, and currently is, contributorily infringing the ’537 Patent, in violation of 35 U.S.C. § 271(c).

39. For similar reasons, Dropbox also infringes the ’537 Patent by supplying or causing to be supplied in or from the United States all or a substantial portion of the components of the Accused Instrumentalities, where such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the ’537 Patent if such combination occurred within the United States. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., storage and metadata servers) and software (e.g., Dropbox Business software) components of the Accused Instrumentalities in such a manner as to actively induce the combination of such components (e.g., by instructing users to rely on multiple servers that save redundant copies of metadata and content in a typical Dropbox Business system) outside of the United States.

40. Dropbox also indirectly infringes the ’537 Patent by supplying or causing to be supplied in or from the United States components of the Accused Instrumentalities that are especially made or especially adapted for use in infringing the ’537 Patent and are not a staple article or commodity of commerce suitable for substantial non-infringing use, and where such components are uncombined in whole or in part, knowing that such components are so made or adapted and intending that such components are combined outside of the United States in a manner that would infringe the ’537 Patent if such combination occurred within the United States. Because the Accused Instrumentalities are designed to operate as the claimed system and apparatus, the Accused Instrumentalities have no substantial non-infringing uses, and any other uses would be unusual, far-fetched, illusory, impractical, occasional, aberrant, or experimental. For

example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., separate Storage servers and Metadata servers) and software (e.g., Dropbox Business software) components that are especially made or especially adapted for use in the Accused Instrumentalities, where such hardware and software components are not staple articles or commodities of commerce suitable for substantial noninfringing use, knowing that such components are so made or adapted and intending that such components are combined outside of the United States, as evidenced by Dropbox's own actions or instructions to users, and enabling and configuring the infringing functionalities of the Accused Instrumentalities.

41. As a result of Defendant's infringement of the '537 Patent, Plaintiff Data Scape is entitled to monetary damages in an amount adequate to compensate for Dropbox's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dropbox, together with interest and costs as fixed by the Court.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 8,386,581

42. Data Scape is the owner by assignment of United States Patent No. 8,386,581 ("the '581 Patent"), entitled "Communication System And Its Method and Communication Apparatus And Its Method." The '581 Patent was duly and legally issued by the United States Patent and Trademark Office on February 26, 2013. A true and correct copy of the '581 Patent is included as Exhibit C.

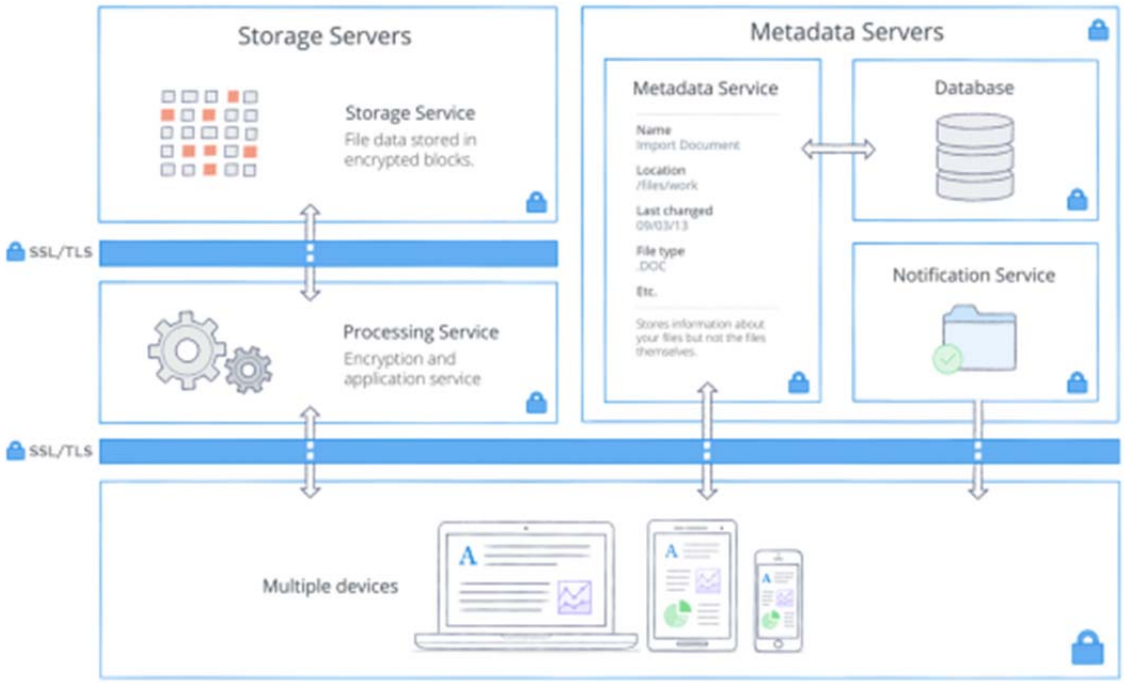
43. Dropbox has offered for sale, sold and/or imported into the United States products and services that infringe the '581 patent, and continues to do so. By way of illustrative example, these infringing products and services include, without limitation,

Defendant's products and services, *e.g.*, Dropbox software, and all versions and variations thereof since the issuance of the '581 Patent ("Accused Instrumentalities").

44. Dropbox has directly infringed and continues to infringe the '581 Patent, for example, by making, selling, offering for sale, and/or importing the Accused Instrumentalities, and through its own use and testing of the Accused Instrumentalities. Dropbox uses the Accused Instrumentalities for its own internal non-testing business purposes, while testing the Accused Instrumentalities, and while providing technical support for the Accused Instrumentalities to its customers.

45. For example, the Accused Instrumentalities infringe Claim 1 (as well as other claims) of the '581 Patent. One non-limiting example of the Accused Instrumentalities' infringement is presented below:

46. The Accused Instrumentalities include "[a] communication apparatus." For example, the Accused Instrumentalities communicate data stored on one device (e.g. a Dropbox storage server) to another device(e.g. a user device with the Dropbox desktop app installed). *See, e.g.*, "Dropbox Business Security" *available at* https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf:

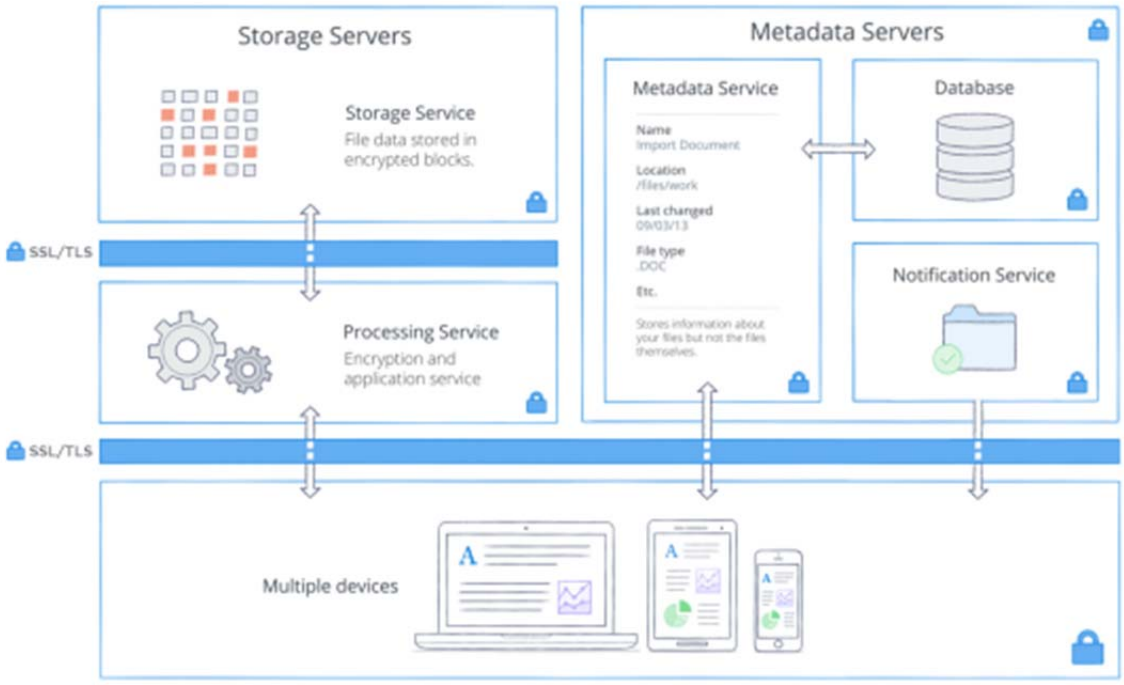


47. The Accused Instrumentalities include a communication apparatus comprising "a storage unit configured to store content data to a storage medium." For example, Dropbox Business includes a storage unit configured to store content data (e.g. files) to a storage medium (e.g. Storage Servers). *See, e.g.*, "Dropbox Business Security" at 5:

File data storage

Dropbox stores metadata about files (such as the date and time a file was last changed) and the actual contents of files (file blocks). File metadata is stored on Dropbox servers. File content is stored in one of two systems: Amazon Web Services (AWS) or Magic Pocket, Dropbox's in-house storage system. Magic Pocket consists of both proprietary software and hardware and has been designed from the ground up to be reliable and secure. In both Magic Pocket and AWS, file blocks are encrypted at rest, and both systems meet high standards for reliability. For more details, please see the **Reliability** section below.

48. The Accused Instrumentalities further include "a communication unit configured to communicate with an external apparatus." For example, Dropbox Business provides a communication unit (e.g. a unit that makes use of SSL/TLS) configured to communicate with an external apparatus (e.g. a user device). *See, e.g.*, "Dropbox Business Security" at 4, 5:



Sync

Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

- **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
- **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
- **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

49. The Accused Instrumentalities further include a communication apparatus comprising "a controller configured to edit a list so that content data is registered in the

list." For example, Dropbox Business provides a controller configured to edit a list (e.g. a list of files or folders in a particular account) so that content data (e.g. files or folders) is registered in the list. *See, e.g.*, "Smart Sync for Team Admins" *available at* https://www.dropbox.com/help/desktop-web/smart-sync-admins:

> Smart Sync helps you and your team share content without worrying about overloading your hard drives. Smart Sync team settings are available to Dropbox Business team admins.
>
> When your team starts using Smart Sync, content that's already downloaded to team member devices remains downloaded. New content is automatically online-only unless you change this setting in the Admin Console. Team members can also chose a personal default for each of their connected computers.
>
> The Smart Sync default applies to new content after the default is enabled and isn't retroactive. The Smart Sync default applies to:
>
> - Joining a shared folder
> - Linking a new device
> - Adding new content from another computer
>
> To set a default for your team:
>
> 1. Sign in to dropbox.com with your admin account.
> 2. Click **Admin Console**.
> 3. Click **Settings**.
> 4. Click **Smart Sync**.
> 5. Select a default for Smart Sync:
>
>   - Synced locally
>   - Online-only

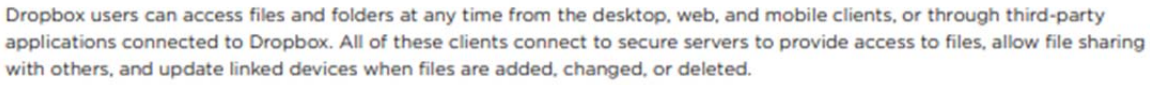
See also "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:

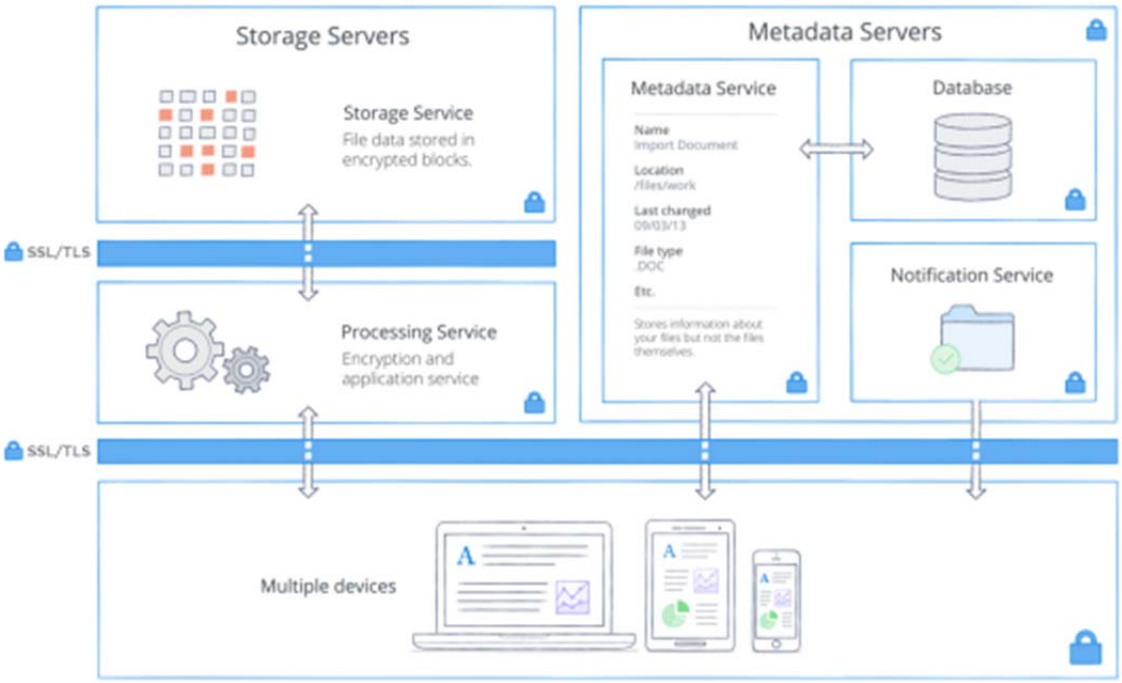
> Smart Sync is a Dropbox feature that helps you save space on your hard drive. Access every file and folder in your Dropbox account from your computer, using virtually no hard drive space. Smart Sync is available for Dropbox Professional customers, and members of Dropbox Business teams. With Smart Sync, you can:
>
> - Choose if individual files or folders are available online-only or locally on your computer
> - Select a default sync setting for new files and folders that are shared with you

50. The Accused Instrumentalities further include a communication apparatus comprising a controller configured "to uniquely associate the list with the external apparatus using a unique identification of the external apparatus." For example, Dropbox Business includes a controller configured to uniquely associate the list with the external apparatus using a unique identification of the external apparatus. *See, e.g.*, "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:

> Smart Sync is a Dropbox feature that helps you save space on your hard drive. Access every file and folder in your Dropbox account from your computer, using virtually no hard drive space. Smart Sync is available for Dropbox Professional customers, and members of Dropbox Business teams. With Smart Sync, you can:
>
> - Choose if individual files or folders are available online-only or locally on your computer
> - Select a default sync setting for new files and folders that are shared with you

51. The Accused Instrumentalities further include a communication apparatus comprising a controller configured "to extract the list associated with the external apparatus from a plurality of lists in the communication apparatus when the external apparatus is connected to the communication apparatus." For example, Dropbox Business includes a controller configured to extract the list (e.g. when updating linked devices when files are added, changed, or deleted) associated with the external apparatus (e.g. user device) from a plurality of lists in the communication apparatus when the external apparatus is connected to the communication apparatus. *See, e.g.*, "Dropbox Business Security" at 3-5:




Storage Servers
Storage Service
File data stored in encrypted blocks.
SSL/TLS
Processing Service
Encryption and application service
SSL/TLS
Multiple devices
Metadata Servers
Metadata Service
Name
Import Document
Location
/files/work
Last changed
09/03/13
File type
.DOC
Etc.
Stores information about your files but not the files themselves.
Database
Notification Service

Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

Sync

Dropbox offers industry-recognized best-in-class file sync. Our sync mechanisms ensure fast, responsive file transfers and enable anywhere access to data across devices. Dropbox is also resilient. In the event of a failed connection to the Dropbox service, a client will gracefully resume operation when a connection is reestablished. Files will only be updated on the local client if they have synchronized completely and successfully validated with the Dropbox service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

- **Delta sync.** Using this sync method, only modified portions of files are downloaded/uploaded. Dropbox stores each file in discrete, encrypted blocks and only updates the blocks that have changed.
- **Streaming sync.** Instead of waiting for a file upload to complete, streaming sync will begin downloading to a second device before files have finished uploading from the first device. This is automatically employed when separate computers are linked to the same Dropbox account or when different Dropbox accounts share a folder.
- **LAN sync.** When enabled, this feature downloads new and updated files from other computers on the same Local Area Network (LAN), saving time and bandwidth compared to downloading the files from Dropbox servers.

52. The Accused Instrumentalities further include a communication apparatus comprising a controller configured "to control transferring of content data registered in the extracted list to the external apparatus." For example, Dropbox Business includes a controller configured to control transferring of content data registered in the extracted list to the external apparatus (e.g. linked user device). *See, e.g.*, "Dropbox Business Security" at 3-5:

Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

See also "Smart Sync" *available at* https://www.dropbox.com/help/desktop-web/smart-sync:

With Smart Sync, content on your computer is available as either online-only, local, or in mixed state folders.

Online-only content

Online-only content appears in the Dropbox folder on your computer, but doesn't use the full amount of space that the file otherwise would. You can see the file, but the content isn't fully downloaded until you need it. Only information about the file, such as the file name, location, and date the file was updated, is downloaded.

Local content

Local content is downloaded and saved on the hard drive of your computer. You can directly edit these files from applications on your computer. This content is still backed up to Dropbox as well.

Mixed state folders

Mixed state folders contain both local and online-only content.

53. Dropbox has had knowledge of the '581 Patent and its infringement since at least the filing of the original Complaint in this action, or shortly thereafter, including by way of this lawsuit. By the time of trial, Dropbox will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of the claims of the ''581 Patent.

54. Dropbox's affirmative acts of making, using, selling, offering for sale, and/or importing the Accused Instrumentalities have induced and continue to induce users of the Accused Instrumentalities to use the Accused Instrumentalities in their

normal and customary way to infringe the claims of the ’581 Patent. Use of the Accused Instrumentalities in their ordinary and customary fashion results in infringement of the claims of the ’581 Patent.

55. For example, Dropbox explains to customers the benefits of using the Accused Instrumentalities, such as by touting their advantages of saving space on hard drives and maintaining access to stored files without using hard drive space in the case of the Dropbox Business feature named “Smart Sync.” Dropbox also induces its customers to use the Accused Instrumentalities to infringe other claims of the ’581 Patent. Dropbox specifically intended and was aware that the normal and customary use of the Accused Instrumentalities on compatible systems would infringe the ’581 Patent. Dropbox performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ’581 Patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Dropbox engaged in such inducement to promote the sales of the Accused Instrumentalities, *e.g.*, through its user manuals, product support, marketing materials, demonstrations, installation support, and training materials to actively induce the users of the accused products to infringe the ’581 Patent. Accordingly, Dropbox has induced and continues to induce end users of the accused products to use the accused products in their ordinary and customary way with compatible systems to make and/or use systems infringing the ’581 Patent, knowing that such use of the Accused Instrumentalities with compatible systems will result in infringement of the ’581 Patent. Accordingly, Dropbox has been (since at least as of filing of the original complaint), and currently is, inducing infringement of the ’581 Patent, in violation of 35 U.S.C. § 271(b).

56. Dropbox has also infringed, and continues to infringe, claims of the ’581 Patent by offering to commercially distribute, commercially distributing, making, and/or importing the Accused Instrumentalities, which are used in practicing the process, or using the systems, of the ’581 Patent, and constitute a material part of the invention. Defendant knows the components in the Accused Instrumentalities to be especially made or especially adapted for use in infringement of the ’581 Patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. For example, the ordinary way of using the Accused Instrumentalities infringes the patent claims, and as such, is especially adapted for use in infringement. Accordingly, Dropbox has been, and currently is, contributorily infringing the ’581 Patent, in violation of 35 U.S.C. § 271(c).

57. For similar reasons, Dropbox also infringes the ’581 Patent by supplying or causing to be supplied in or from the United States all or a substantial portion of the components of the Accused Instrumentalities, where such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the ’581 Patent if such combination occurred within the United States. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., storage and metadata servers) and software (e.g., Dropbox Business software) components of the Accused Instrumentalities in such a manner as to actively induce the combination of such components (e.g., by instructing users to rely on multiple servers that save redundant copies of metadata and content in a typical Dropbox Business system) outside of the United States.

58. Dropbox also indirectly infringes the ’581 Patent by supplying or causing to be supplied in or from the United States components of the Accused Instrumentalities that are especially made or especially adapted for use in infringing the ’581 Patent and are not a staple article or commodity of commerce suitable for substantial non-infringing use, and where such components are uncombined in whole or in part, knowing that such components are so made or adapted and intending that such components are combined outside of the United States in a manner that would infringe the ’581 Patent if such combination occurred within the United States. Because the Accused Instrumentalities are designed to operate as the claimed system and apparatus, the Accused Instrumentalities have no substantial non-infringing uses, and any other uses would be unusual, far-fetched, illusory, impractical, occasional, aberrant, or experimental. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., separate Storage servers and Metadata servers) and software (e.g., Dropbox Business software) components that are especially made or especially adapted for use in the Accused Instrumentalities, where such hardware and software components are not staple articles or commodities of commerce suitable for substantial noninfringing use, knowing that such components are so made or adapted and intending that such components are combined outside of the United States, as evidenced by Dropbox’s own actions or instructions to users and enabling and configuring the infringing functionalities of the Accused Instrumentalities.

59. As a result of Defendant’s infringement of the ’581 Patent, Plaintiff Data Scape is entitled to monetary damages in an amount adequate to compensate for

Dropbox's infringement, but in no event less than a reasonable royalty for the use made of the invention by Dropbox, together with interest and costs as fixed by the Court.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 9,715,893

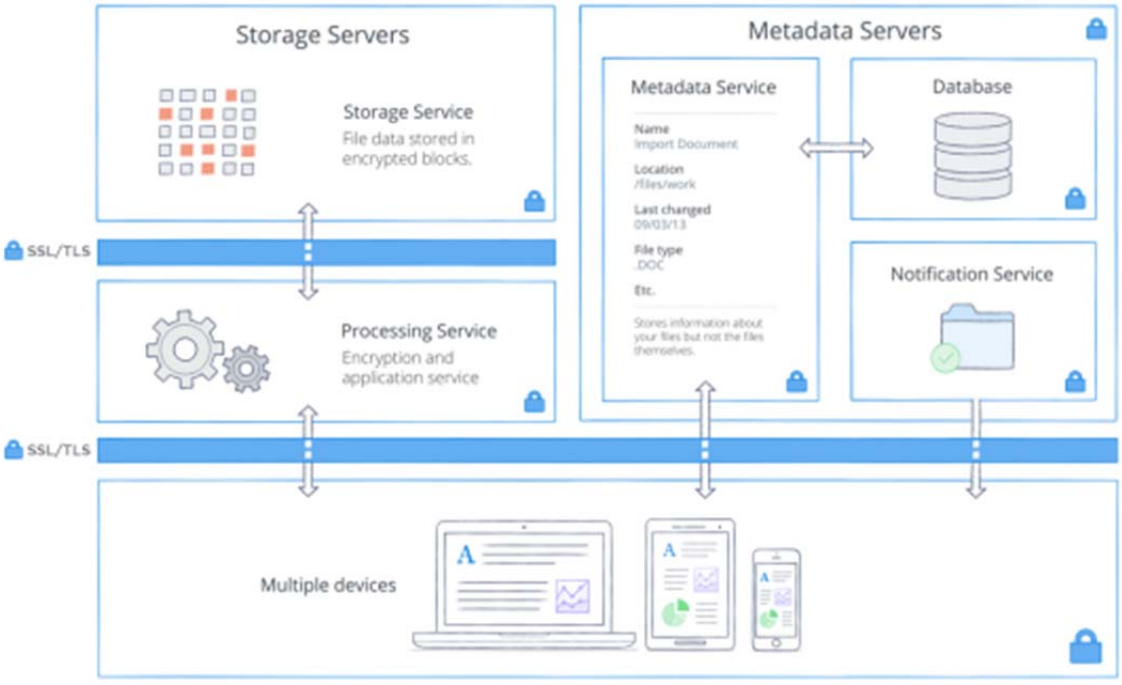
60. Data Scape is the owner by assignment of United States Patent No. 9,715,893 ("the '893 Patent"), entitled "Recording Apparatus, Server Apparatus, Recording Method, Program and Storage Medium." The '893 Patent was duly and legally issued by the United States Patent and Trademark Office on July 25, 2017. A true and correct copy of the '893 Patent is included as Exhibit D.

61. Dropbox has offered for sale, sold and/or imported into the United States products and services that infringe the '893 patent, and continues to do so. By way of illustrative example, these infringing products and services include, without limitation, Defendant's products and services, *e.g.*, Dropbox services, including Dropbox Business, and all versions and variations thereof since the issuance of the '893 Patent ("Accused Instrumentalities").

62. Dropbox has directly infringed and continues to infringe the '893 Patent, for example, by making, selling, offering for sale, and/or importing the Accused Instrumentalities, and through its own use and testing of the Accused Instrumentalities. Dropbox uses the Accused Instrumentalities for its own internal non-testing business purposes, while testing the Accused Instrumentalities, and while providing technical support and repair services for the Accused Instrumentalities to its customers.

63. For example, the Accused Instrumentalities infringe Claim 1 (as well as other claims) of the '893 Patent. One non-limiting example of the Accused Instrumentalities' infringement is presented below:

64. The Accused Instrumentalities include "[a] non-transitory computer-readable storage medium storing instructions which, when executed by a computer, cause the computer to perform a method of an information processing apparatus for transferring data." Dropbox Business includes instructions for transferring data from Dropbox Business storage servers to a user device with the Dropbox app installed. *See*, *e.g.*, "Dropbox Business Security" *available at* https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vfllunodj.pdf:



65. The Accused Instrumentalities include instructions for "automatically reading first management data from a first storage medium, the first management data

identifying files of source data stored on the first storage medium." For example, Dropbox Business includes a Metadata service that stores metadata about files (such as the date and time a file was last changed) and acts as an index for data stored in user accounts. *See, e.g.*, "Dropbox Business Security" at 3-5:

> Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.
>
> Our architecture is comprised of the following services:
>
> - **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
> - **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
> - **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
> - **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

66. The Accused Instrumentalities include instructions for "automatically identifying, by the computer, one of the files of source data based on the first management data and second management data, the second management data identifying files of transferred data stored on a second storage medium, the one of the files of source data being absent from the second storage medium." For example, Dropbox Business includes a Notification service that, if a change to a stored file occurs or if a new file is created anywhere in the Dropbox Business system, informs linked devices of the change. *See, e.g.*, "Dropbox Business Security" at 3-5:

Dropbox users can access files and folders at any time from the desktop, web, and mobile clients, or through third-party applications connected to Dropbox. All of these clients connect to secure servers to provide access to files, allow file sharing with others, and update linked devices when files are added, changed, or deleted.

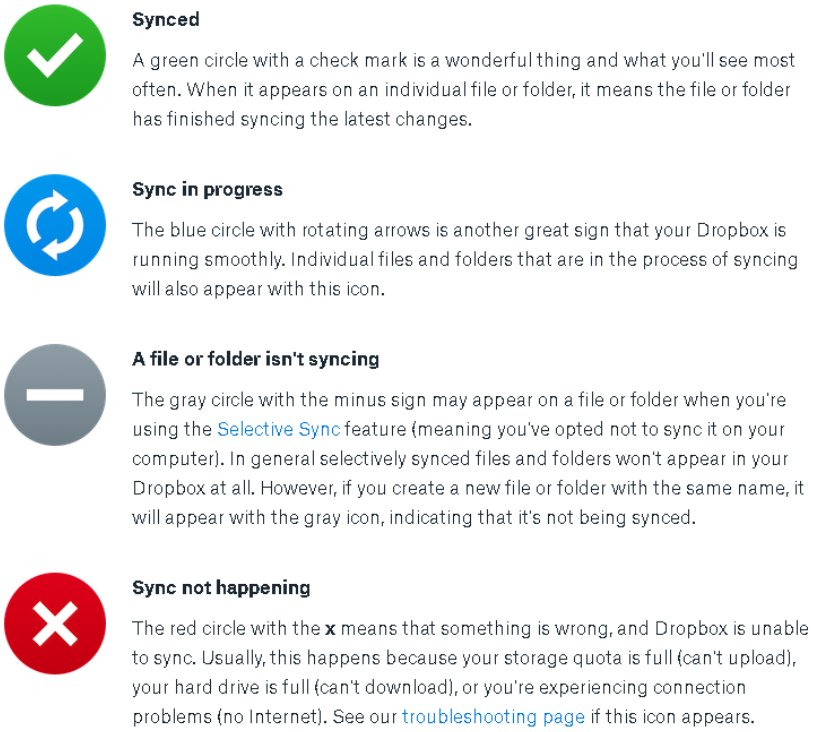
Our architecture is comprised of the following services:

- **Processing service.** By design, Dropbox provides a unique security mechanism that goes beyond traditional encryption to protect user data. The Encryption and Application Services process files from the Dropbox applications by splitting each into blocks, encrypting each file block using a strong cipher, and synchronizing only blocks that have been modified between revisions. When a Dropbox application detects a new file or changes to an existing file, the application notifies the encryption and application services of the change, and new or modified file blocks are processed and transferred to the storage service. For detailed information on the encryption used by these services both in transit and at rest, please see the Encryption section below.
- **Storage service.** The actual contents of users' files are stored in encrypted blocks with this service. Prior to transmission, the Dropbox client splits files into file blocks in preparation for the block storage service. The storage service acts as a Content-Addressable Storage (CAS) system, with each individual encrypted file block retrieved based on its hash value.
- **Metadata service.** Certain basic information about user data (including file names and types), called metadata, is kept in its own discrete storage service and acts as an index for the data in users' accounts. Dropbox metadata is stored in a MySQL-backed database service, and is sharded and replicated as needed to meet performance and high availability requirements. Metadata includes basic account and user information, like email address, name, and device names. Metadata also includes basic information about files, including file names and types, that helps support features like version history, recovery, and sync.
- **Notification service.** This separate service is dedicated to monitoring whether or not any changes have been made to Dropbox accounts. No files or metadata are stored here or transferred. Each client establishes a long poll connection to the notification service and waits. When a change to any file in Dropbox takes place, the notification service signals a change to the relevant client(s) by closing the long poll connection. Closing the connection signals that the client must connect to the metadata service securely to synchronize any changes.

67. The Accused Instrumentalities include instructions for "automatically transferring the one of the files of source data to the second storage medium, the one of the files of source data being transferred becoming one of the files of transferred data." For example, Dropbox Business will automatically update linked devices when shared files are added, changed, or deleted elsewhere in the Dropbox Business system.

68. The Accused Instrumentalities include instructions for "automatically displaying transferring status of the one of the files of source data by a symbolic figure." For example, Dropbox Business automatically displays status icons for the status of a sync operation. *See, e.g.*, "The sync icons on files in the desktop app" *available at* https://www.dropbox.com/help/syncing-uploads/icon-overlays-not-appearing:

Status icons for files



Synced

A green circle with a check mark is a wonderful thing and what you'll see most often. When it appears on an individual file or folder, it means the file or folder has finished syncing the latest changes.

Sync in progress

The blue circle with rotating arrows is another great sign that your Dropbox is running smoothly. Individual files and folders that are in the process of syncing will also appear with this icon.

A file or folder isn't syncing

The gray circle with the minus sign may appear on a file or folder when you're using the Selective Sync feature (meaning you've opted not to sync it on your computer). In general selectively synced files and folders won't appear in your Dropbox at all. However, if you create a new file or folder with the same name, it will appear with the gray icon, indicating that it's not being synced.

Sync not happening

The red circle with the **x** means that something is wrong, and Dropbox is unable to sync. Usually, this happens because your storage quota is full (can't upload), your hard drive is full (can't download), or you're experiencing connection problems (no Internet). See our troubleshooting page if this icon appears.

69. Dropbox has had knowledge of the '893 Patent and its infringement since at least the filing of the original Complaint in this action, or shortly thereafter, including by way of this lawsuit. By the time of trial, Dropbox will have known and intended (since receiving such notice) that its continued actions would actively induce and contribute to the infringement of the claims of the '893 Patent.

70. Dropbox's affirmative acts of making, using, selling, offering for sale, and/or importing the Accused Instrumentalities have induced and continue to induce users of the Accused Instrumentalities to use the Accused Instrumentalities in their normal and customary way to infringe the claims of the '893 Patent. Use of the Accused Instrumentalities in their ordinary and customary fashion results in infringement of the claims of the '893 Patent.

71. For example, Dropbox explains to customers the benefits of using the Accused Instrumentalities, such as by touting their advantages of replicating data among multiple devices. Dropbox also induces its customers to use the Accused Instrumentalities to infringe other claims of the '893 Patent. Dropbox specifically intended and was aware that the normal and customary use of the Accused Instrumentalities on compatible systems would infringe the '893 Patent. Dropbox performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '893 Patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Dropbox engaged in such inducement to promote the sales of the Accused Instrumentalities, *e.g.*, through its user manuals, product support, marketing materials, demonstrations, installation support, and training materials to actively induce the users of the accused products to infringe the '893 Patent. Accordingly, Dropbox has induced and continues to induce end users of the accused products to use the accused products in their ordinary and customary way with compatible systems to make and/or use systems infringing the '893 Patent, knowing that such use of the Accused Instrumentalities with compatible systems will result in infringement of the '893 Patent. Accordingly, Dropbox has been (since at least as of filing of the original complaint), and currently is, inducing infringement of the '893 Patent, in violation of 35 U.S.C. § 271(b).

72. Dropbox has also infringed, and continues to infringe, claims of the '893 Patent by offering to commercially distribute, commercially distributing, making, and/or importing the Accused Instrumentalities, which are used in practicing the process, or using the systems, of the '893 Patent, and constitute a material part of the invention.

Defendant knows the components in the Accused Instrumentalities to be especially made or especially adapted for use in infringement of the ’893 Patent, not a staple article, and not a commodity of commerce suitable for substantial noninfringing use. For example, the ordinary way of using the Accused Instrumentalities infringes the patent claims, and as such, is especially adapted for use in infringement. Accordingly, Dropbox has been, and currently is, contributorily infringing the ’893 Patent, in violation of 35 U.S.C. § 271(c).

73. For similar reasons, Dropbox also infringes the ’893 Patent by supplying or causing to be supplied in or from the United States all or a substantial portion of the components of the Accused Instrumentalities, where such components are uncombined in whole or in part, in such manner as to actively induce the combination of such components outside of the United States in a manner that would infringe the ’893 Patent if such combination occurred within the United States. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., storage and metadata servers) and software (e.g., Dropbox Business software) components of the Accused Instrumentalities in such a manner as to actively induce the combination of such components (e.g., by instructing users to rely on multiple servers that save redundant copies of metadata and content in a typical Dropbox Business system) outside of the United States.

74. Dropbox also indirectly infringes the ’893 Patent by supplying or causing to be supplied in or from the United States components of the Accused Instrumentalities that are especially made or especially adapted for use in infringing the ’893 Patent and are not a staple article or commodity of commerce suitable for substantial non-infringing

use, and where such components are uncombined in whole or in part, knowing that such components are so made or adapted and intending that such components are combined outside of the United States in a manner that would infringe the ’893 Patent if such combination occurred within the United States. Because the Accused Instrumentalities are designed to operate as the claimed system and apparatus, the Accused Instrumentalities have no substantial non-infringing uses, and any other uses would be unusual, far-fetched, illusory, impractical, occasional, aberrant, or experimental. For example, Dropbox supplies or causes to be supplied in or from the United States all or a substantial portion of the hardware (e.g., separate Storage servers and Metadata servers) and software (e.g., Dropbox Business software) components that are especially made or especially adapted for use in the Accused Instrumentalities, where such hardware and software components are not staple articles or commodities of commerce suitable for substantial noninfringing use, knowing that such components are so made or adapted and intending that such components are combined outside of the United States, as evidenced by Dropbox’s own actions or instructions to users, and enabling and configuring the infringing functionalities of the Accused Instrumentalities.

75. As a result of Defendant’s infringement of the ’893 Patent, Plaintiff Data Scape is entitled to monetary damages in an amount adequate to compensate for Dropbox’s infringement, but in no event less than a reasonable royalty for the use made of the invention by Dropbox, together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Data Scape respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that Dropbox has infringed, either literally and/or under the doctrine of equivalents, the ’581 Patent, ’929 Patent, the ’537 Patent, and the ’893 Patent (collectively, “asserted patents”);

b. A permanent injunction prohibiting Dropbox from further acts of infringement of the asserted patents;

c. A judgment and order requiring Dropbox to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for its infringement of the asserted patents, as provided under 35 U.S.C. § 284;

d. A judgment and order requiring Dropbox to provide an accounting and to pay supplemental damages to Data Scape, including without limitation, prejudgment and post-judgment interest;

e. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys’ fees against Dropbox; and

f. Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: January 25, 2019 Respectfully submitted,

/s/
Marc A. Fenster (CA SBN 181067)
Reza Mirzaie (CA SBN 246953)
Brian D. Ledahl (CA SBN 186579)
Paul Kroeger (CA SBN 229074)
C. Jay Chung (CA SBN 252794)
Philip X. wang (CA SBN 262239)
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
(310) 826-7474
mfenster@raklaw.com
rmirzaie@raklaw.com
bledahl@raklaw.com
pkroeger@raklaw.com
jchung@raklaw.com
pwang@raklaw.com
Attorneys for Plaintiff Data Scape Limited