UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

REALTIME DATA LLC d/b/a IXO, Plaintiff, v. ACRONIS, INC., Defendant.	Case No. 1:17-cv-11279-IT **JURY TRIAL DEMANDED**

AMENDED COMPLAINT FOR PATENT INFRINGEMENT AGAINST ACRONIS, INC.

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 Realtime Data LLC d/b/a IXO ("Plaintiff," "Realtime," or "IXO") makes the following allegations against Defendant Acronis, Inc. ("Acronis"):

PARTIES

1. Realtime is a limited liability company organized under the laws of the State of New York. Realtime has places of business at 5851 Legacy Circle, Plano, Texas 75024, 1828 E.S.E. Loop 323, Tyler, Texas 75701, and 66 Palmer Avenue, Suite 27, Bronxville, NY 10708. Since the 1990s, Realtime has researched and developed specific solutions for data compression, including, for example, those that increase the speeds at which data can be stored and accessed. As recognition of its innovations rooted in this technological field, Realtime holds 47 United States patents and has numerous pending patent applications. Realtime has licensed patents in this portfolio to many of the world's leading technology companies. The patents-in-suit relate to Realtime's development of advanced systems and methods for fast and efficient data compression using numerous innovative compression techniques based on, for example, particular attributes of the data.

2. On information and belief, Defendant Acronis Inc. ("Acronis") is a Delaware corporation with its principal place of business at 1 Van de Graaff Drive, Suite 301, Burlington, MA, 01803. On information and belief, Acronis can be served through its registered agent, Corporation Service Company, 2711 Centerville Rd Suite 400, 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 Defendant Acronis in this action because Acronis has committed acts within the District of Massachusetts giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Acronis would not offend traditional notions of fair play and substantial justice. Acronis, 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, Acronis has transacted business in the District of Massachusetts, has committed acts of direct and indirect infringement in this District, and has a regular and established place of business in this District.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 9,054,728

6. Plaintiff realleges and incorporates by reference paragraphs 1-5 above, as if fully set forth herein.

7. Plaintiff Realtime is the owner by assignment of United States Patent No. 9,054,728 ("the '728 patent") entitled "Data compression systems and methods." The '728

patent was duly and legally issued by the United States Patent and Trademark Office on June 9, 2015. A true and correct copy of the '728 Patent is included as Exhibit A.

8. On information and belief, Acronis has offered for sale, sold and/or imported into the United States Acronis products that infringe the '728 patent, and continues to do so. By way of illustrative example, these infringing products include, without limitation, Acronis's products and services, e.g., Acronis Backup Advanced, including version 11.7 thereof, and all versions and variations thereof since the issuance of the '728 patent ("Accused Instrumentality").

9. On information and belief, Acronis has directly infringed and continues to infringe the '728 patent, for example, through its own use and testing of the Accused Instrumentality, which constitute systems for compressing data claimed by Claim 1 of the '728 patent, comprising a processor; one or more content dependent data compression encoders; and a single data compression encoder; wherein the processor is configured: to analyze data within a data block to identify one or more parameters or attributes of the data wherein the analyzing of the data within the data block to identify the one or more parameters or attributes of the data excludes analyzing based solely on a descriptor that is indicative of the one or more parameters or attributes of the data within the data block; to perform content dependent data compression with the one or more content dependent data compression encoders if the one or more parameters or attributes of the data are identified; and to perform data compression with the single data compression encoder, if the one or more parameters or attributes of the data are not identified. Upon information and belief, Acronis uses the Accused Instrumentality, an infringing system, for its own internal non-testing business purposes, while testing the Accused Instrumentality, and while providing technical support and repair services for the Accused Instrumentality to Acronis's customers.

10. On information and belief, Acronis has had knowledge of the '728 patent since at least the filing of this Complaint or shortly thereafter, and on information and belief, Acronis knew of the '728 patent and knew of its infringement, including by way of this lawsuit.

11. Acronis's affirmative acts of making, using, selling, offering for sale, and/or importing the Accused Instrumentality has induced and continues to induce users of the Accused Instrumentality to use the Accused Instrumentality in its normal and customary way on compatible systems to infringe the '728 patent, knowing that when the Accused Instrumentality is used in its ordinary and customary manner with such compatible systems, such systems constitute infringing systems for compressing data comprising; a processor; one or more content dependent data compression encoders; and a single data compression encoder; wherein the processor is configured: to analyze data within a data block to identify one or more parameters or attributes of the data wherein the analyzing of the data within the data block to identify the one or more parameters or attributes of the data excludes analyzing based solely on a descriptor that is indicative of the one or more parameters or attributes of the data within the data block; to perform content dependent data compression with the one or more content dependent data compression encoders if the one or more parameters or attributes of the data are identified; and to perform data compression with the single data compression encoder, if the one or more parameters or attributes of the data are not identified. For example, Acronis explains to customers the benefits of using the Accused Instrumentality: "One of the key capabilities of the Acronis storage node is deduplication. Deduplication technology helps reduce storage costs and network bandwidth utilization by eliminating duplicate data blocks when you back up and transfer data. Acronis Backup Advanced deduplication helps you to: 1. Reduce storage space usage by storing only unique data 2. Eliminate the need to invest in data deduplication-specific hardware 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks." See http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2. Acronis specifically intended and was aware that the normal and customary use of the Accused Instrumentality on compatible systems would infringe the '728 patent. Acronis performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '728 patent and with the knowledge, or willful blindness to the probability, that

the induced acts would constitute infringement. On information and belief, Acronis engaged in such inducement to promote the sales of the Accused Instrumentality, *e.g.,* through Acronis's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '728 patent. Accordingly, Acronis 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 '728 patent, knowing that such use of the Accused Instrumentality with compatible systems will result in infringement of the '728 patent.

12. Acronis also indirectly infringes the '728 patent by manufacturing, using, selling, offering for sale, and/or importing the accused products, with knowledge that the accused products were and are especially manufactured and/or especially adapted for use in infringing the '728 patent and are not a staple article or commodity of commerce suitable for substantial non-infringing use. On information and belief, the Accused Instrumentality is designed to function with compatible hardware to create systems for compressing data comprising; a processor; one or more content dependent data compression encoders; and a single data compression encoder; wherein the processor is configured: to analyze data within a data block to identify one or more parameters or attributes of the data wherein the analyzing of the data within the data block to identify the one or more parameters or attributes of the data excludes analyzing based solely on a descriptor that is indicative of the one or more parameters or attributes of the data within the data block; to perform content dependent data compression with the one or more content dependent data compression encoders if the one or more parameters or attributes of the data are identified; and to perform data compression with the single data compression encoder, if the one or more parameters or attributes of the data are not identified. Because the Accused Instrumentality is designed to operate as the claimed system for compressing input data, the Accused Instrumentality has no substantial non-infringing uses, and any other uses would be unusual, far-fetched, illusory, impractical, occasional, aberrant, or experimental. Acronis's manufacture, use,

sale, offering for sale, and/or importation of the Accused Instrumentality constitutes contributory infringement of the '728 patent.

13. The Accused Instrumentality is a system for compressing data, comprising a processor. For example, the Accused Instrumentality must run on hardware containing a processor. See, e.g., http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 16 ("Use a minimum of 2.5 GHz CPU with at least four cores. Multi-CPU systems are also supported.").

14. The Accused Instrumentality is a system for compressing data, comprising one or more content dependent data compression encoders. For example, the Accused Instrumentality performs deduplication, which is a content dependent data compression encoder. Performing deduplication results in representation of data with fewer bits. See, e.g., http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself.").

15. The Accused Instrumentality comprises a single data compression encoder. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 10 ("The Acronis Backup agent compresses the backed up data before sending it to the server.").

16. The Accused Instrumentality analyzes data within a data block to identify one or more parameters or attributes of the data, for example, whether the data is duplicative of data previously transmitted and/or stored, where the analysis does not rely only on the descriptor. *See,*

e.g., http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself.").

17. The Accused Instrumentality performs content dependent data compression with the one or more content dependent data compression encoders if the one or more parameters or attributes of the data are identified. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself.").

18. The Accused Instrumentality performs data compression with the single data compression encoder, if the one or more parameters or attributes of the data are not identified. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 10 ("The Acronis Backup agent compresses the backed up data before sending it to the server. Hash values for each data block are calculated before compression. If two equal blocks are compressed with different levels of compression, they are still recognized as duplicates.").

19. Acronis also infringes other claims of the '728 patent, directly and through inducing infringement and contributory infringement, for similar reasons as explained above with respect to Claim 1 of the '728 patent.

20. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentality, and touting the benefits of using the Accused Instrumentality's compression features, Acronis has injured Realtime and is liable to Realtime for infringement of the '728 patent pursuant to 35 U.S.C. § 271.

21. As a result of Acronis's infringement of the '728 patent, Plaintiff Realtime is entitled to monetary damages in an amount adequate to compensate for Acronis's infringement, but in no event less than a reasonable royalty for the use made of the invention by Acronis, together with interest and costs as fixed by the Court.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 7,415,530

22. Plaintiff realleges and incorporates by reference paragraphs 1-21 above, as if fully set forth herein.

23. Plaintiff Realtime is the owner by assignment of United States Patent No. 7,415,530 ("the '530 patent") entitled "System and methods for accelerated data storage and retrieval." The '530 patent was duly and legally issued by the United States Patent and Trademark Office on August 19, 2008. A true and correct copy of the '530 patent is included as Exhibit B.

24. On information and belief, Acronis has offered for sale, sold and/or imported into the United States Acronis products that infringe the '530 patent, and continues to do so. By way of illustrative example, these infringing products include, without limitation, Acronis's products and services, e.g., Acronis Backup Advanced, including version 11.7 thereof, and all versions and variations thereof since the issuance of the '530 patent ("Accused Instrumentality").

25. On information and belief, Acronis has directly infringed and continues to infringe the '530 patent, for example, through its own use and testing of the Accused Instrumentality, which constitutes a system comprising: a memory device; and a data accelerator, wherein said data accelerator is coupled to said memory device, a data stream is received by said data accelerator in received form, said data stream includes a first data block and a second data block, said data stream is compressed by said data accelerator to provide a compressed data stream by compressing said first data block with a first compression technique and said second data block with a second compression technique, said first and second compression techniques are different, said compressed data stream is stored on said memory device, said compression and storage occurs faster than said data stream is able to be stored on said memory device in said received form, a first data descriptor is stored on said memory device indicative of said first compression technique, and said first descriptor is utilized to decompress the portion of said compressed data stream associated with said first data block. Upon information and belief, Acronis uses the Accused Instrumentality, an infringing system, for its own internal non-testing business purposes, while testing the Accused Instrumentality, and while providing technical support and repair services for the Accused Instrumentality to Acronis's customers.

26. On information and belief, Acronis has had knowledge of the '530 patent since at least the filing of this Complaint or shortly thereafter, and on information and belief, Acronis knew of the '530 patent and knew of its infringement, including by way of this lawsuit.

27. Upon information and belief, Acronis's affirmative acts of making, using, and selling the Accused Instrumentalities, and providing implementation services and technical support to users of the Accused Instrumentalities, have induced and continue to induce users of the Accused Instrumentalities to use them in their normal and customary way to infringe Claim 1 of the '530 patent by making or using a system comprising: a memory device; and a data accelerator, wherein said data accelerator is coupled to said memory device, a data stream is received by said data accelerator in received form, said data stream includes a first data block and a second data block, said data stream is compressed by said data accelerator to provide a

compressed data stream by compressing said first data block with a first compression technique and said second data block with a second compression technique, said first and second compression techniques are different, said compressed data stream is stored on said memory device, said compression and storage occurs faster than said data stream is able to be stored on said memory device in said received form, a first data descriptor is stored on said memory device indicative of said first compression technique, and said first descriptor is utilized to decompress the portion of said compressed data stream associated with said first data block. For example, Acronis explains to customers the benefits of using the Accused Instrumentality: "One of the key capabilities of the Acronis storage node is deduplication. Deduplication technology helps reduce storage costs and network bandwidth utilization by eliminating duplicate data blocks when you back up and transfer data. Acronis Backup Advanced deduplication helps you to: 1. Reduce storage space usage by storing only unique data 2. Eliminate the need to invest in data deduplication-specific hardware 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks." See http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2. For similar reasons, Acronis also induces its customers to use the Accused Instrumentalities to infringe other claims of the '530 patent. Acronis specifically intended and was aware that these normal and customary activities would infringe the '530 patent. Acronis performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '530 patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Acronis engaged in such inducement to promote the sales of the Accused Instrumentalities. Accordingly, Acronis has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '530 patent, knowing that such use constitutes infringement of the '530 patent.

28. The Accused Instrumentality evidently includes the memory device and includes the data accelerator, wherein said data accelerator is coupled to said memory device. For

example, the Accused Instrumentality must run on hardware containing a memory device. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 8 ("you should store the deduplication database and deduplication data store on separate disks to achieve better performance.").

29. The Accused Instrumentality receives an incoming stream of data. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 4 ("During deduplication, the backup data is split into blocks. Each block's uniqueness is checked through a special database, which tracks all the stored blocks' checksums. Unique blocks are sent to the storage and duplicates are skipped.").

30. The Accused Instrumentality's received data stream will evidently consist of more than one data block. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 4 ("During deduplication, the backup data is split into blocks. Each block's uniqueness is checked through a special database, which tracks all the stored blocks' checksums. Unique blocks are sent to the storage and duplicates are skipped.").

31. The Accused Instrumentality compresses said data stream to provide a compressed data stream by compressing said first data block with a first compression technique and said second data block with a second compression technique. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5, 10 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself. … The Acronis Backup agent compresses the backed up data before sending it to the server. Hash values for each data block

are calculated before compression. If two equal blocks are compressed with different levels of compression, they are still recognized as duplicates.").

32. The first (deduplication) and second (compression) compression techniques used by the Accused Instrumentality described above are necessarily different. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5, 10 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself. … The Acronis Backup agent compresses the backed up data before sending it to the server. Hash values for each data block are calculated before compression. If two equal blocks are compressed with different levels of compression, they are still recognized as duplicates.").

33. After compression, said compressed data stream is stored on said memory device. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 4 ("Deduplication minimizes storage space by detecting data repetition and storing the identical data only once. Deduplication reduces network load. During a backup, if data is found to be a duplicate of data previously backed up, it is not transferred over the network to storage. … During deduplication, the backup data is split into blocks. Each block's uniqueness is checked through a special database, which tracks all the stored blocks' checksums. Unique blocks are sent to the storage and duplicates are skipped.").

34. Said compression and storage occurs faster than said data stream is able to be stored on said memory device in said received form. See, e.g., http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2 ("Deduplication technology helps reduce storage costs and network bandwidth utilization by

eliminating duplicate data blocks when you back up and transfer data. … Acronis Backup Advanced deduplication helps you to: … 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks.").

35. The Accused Instrumentality would evidently store a first data descriptor on said memory device indicative of said first compression technique, such as a pointer to a deduplicated data block, and utilize said first descriptor to decompress the portion of said compressed data stream associated with said first data block. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5, 8-9 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself. … The Acronis Backup Advanced's Storage Node with a deduplicated vault maintains the deduplication database. The deduplication database contains the hash values of all data blocks stored in the vault, except for those that cannot be deduplicated, e.g., encrypted files. During recovery, the Acronis Backup agent requests the data from the Acronis storage node through a proprietary, secure protocol. The storage node reads backup data from the vault and if a block is referenced in the deduplication data store, the storage node reads data from it. For an agent, the recovery process is transparent and independent of the deduplication.").

36. On information and belief, Acronis also infringes, directly and through induced infringement, and continues to infringe other claims of the '530 patent, for similar reasons as explained above with respect to Claim 1 of the '530 patent.

37. On information and belief, use of the Accused Instrumentality in its ordinary and customary fashion results in infringement of the methods claimed by the '530 patent.

38. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentalities, and touting the benefits of using the Accused Instrumentalities' compression features, Acronis has injured Realtime and is liable to Realtime for infringement of the '530 patent pursuant to 35 U.S.C. § 271.

39. As a result of Acronis's infringement of the '530 patent, Plaintiff Realtime is entitled to monetary damages in an amount adequate to compensate for Acronis's infringement, but in no event less than a reasonable royalty for the use made of the invention by Acronis, together with interest and costs as fixed by the Court.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 9,116,908

40. Plaintiff Realtime realleges and incorporates by reference paragraphs 1-39 above, as if fully set forth herein.

41. Plaintiff Realtime is the owner by assignment of United States Patent No. 9,116,908 ("the '908 Patent") entitled "System and methods for accelerated data storage and retrieval." The '908 Patent was duly and legally issued by the United States Patent and Trademark Office on August 25, 2015. A true and correct copy of the '908 Patent is included as Exhibit C.

42. On information and belief, Acronis has offered for sale, sold and/or imported into the United States Acronis products that infringe the '908 patent, and continues to do so. By way of illustrative example, these infringing products include, without limitation, Acronis's products and services, e.g., Acronis Backup Advanced, including version 11.7 thereof, and all versions and variations thereof since the issuance of the '908 patent ("Accused Instrumentality").

43. On information and belief, Acronis has directly infringed and continues to infringe the '908 patent, for example, through its own use and testing of the Accused Instrumentality, which constitutes a system comprising: a memory device; and a data accelerator configured to compress: (i) a first data block with a first compression technique to provide a first

compressed data block; and (ii) a second data block with a second compression technique, different from the first compression technique, to provide a second compressed data block; wherein the compressed first and second data blocks are stored on the memory device, and the compression and storage occurs faster than the first and second data blocks are able to be stored on the memory device in uncompressed form. Upon information and belief, Acronis uses the Accused Instrumentality, an infringing system, for its own internal non-testing business purposes, while testing the Accused Instrumentality, and while providing technical support and repair services for the Accused Instrumentality to Acronis's customers.

44. On information and belief, use of the Accused Instrumentality in its ordinary and customary fashion results in infringement of the systems claimed by the '908 patent.

45. On information and belief, Acronis has had knowledge of the '908 patent since at least the filing of this Complaint or shortly thereafter, and on information and belief, Acronis knew of the '908 patent and knew of its infringement, including by way of this lawsuit.

46. Upon information and belief, Acronis's affirmative acts of making, using, and selling the Accused Instrumentalities, and providing implementation services and technical support to users of the Accused Instrumentalities, have induced and continue to induce users of the Accused Instrumentalities to use them in their normal and customary way to infringe Claim 1 of the '908 patent by making or using a system comprising: a memory device; and a data accelerator configured to compress: (i) a first data block with a first compression technique to provide a first compressed data block; and (ii) a second data block with a second compression technique, different from the first compression technique, to provide a second compressed data block; wherein the compressed first and second data blocks are stored on the memory device, and the compression and storage occurs faster than the first and second data blocks are able to be stored on the memory device in uncompressed form. For example, Acronis explains to customers the benefits of using the Accused Instrumentality: "One of the key capabilities of the Acronis storage node is deduplication. Deduplication technology helps reduce storage costs and network bandwidth utilization by eliminating duplicate data blocks when you back up and

transfer data. Acronis Backup Advanced deduplication helps you to: 1. Reduce storage space usage by storing only unique data 2. Eliminate the need to invest in data deduplication-specific hardware 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks." See http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2. For similar reasons, Acronis also induces its customers to use the Accused Instrumentalities to infringe other claims of the '908 patent. Acronis specifically intended and was aware that these normal and customary activities would infringe the '908 patent. Acronis performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '908 patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Acronis engaged in such inducement to promote the sales of the Accused Instrumentalities. Accordingly, Acronis has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '908 patent, knowing that such use constitutes infringement of the '908 patent.

47. The Accused Instrumentality evidently includes a memory device and a data accelerator configured to compress: (i) a first data block with a first compression technique to provide a first compressed data block; and (ii) a second data block with a second compression technique, different from the first compression technique, to provide a second compressed data block. For example, the Accused Instrumentality must run on hardware containing a memory device. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 8 ("you should store the deduplication database and deduplication data store on separate disks to achieve better performance."). The Accused Instrumentality compresses (i) a first data block with a first compression technique to provide a first compressed data block; and (ii) a second data block with a second compression technique, different from the first compression technique, to provide a second compressed data block.). *See, e.g.*,

http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5, 10 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself. … The Acronis Backup agent compresses the backed up data before sending it to the server. Hash values for each data block are calculated before compression. If two equal blocks are compressed with different levels of compression, they are still recognized as duplicates.").

48. The Accused Instrumentality stores the compressed first and second data blocks on the memory device, and the compression and storage occurs faster than the first and second data blocks are able to be stored on the memory device in uncompressed form. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2, 4 ("Deduplication technology helps reduce storage costs and network bandwidth utilization by eliminating duplicate data blocks when you back up and transfer data. … Acronis Backup Advanced deduplication helps you to: … 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks. … Deduplication minimizes storage space by detecting data repetition and storing the identical data only once. Deduplication reduces network load. During a backup, if data is found to be a duplicate of data previously backed up, it is not transferred over the network to storage. … During deduplication, the backup data is split into blocks. Each block's uniqueness is checked through a special database, which tracks all the stored blocks' checksums. Unique blocks are sent to the storage and duplicates are skipped.").

49. On information and belief, Acronis also infringes, directly and through induced infringement, and continues to infringe other claims of the '908 patent, for similar reasons as explained above with respect to Claim 1 of the '908 patent.

50. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentalities, and touting the benefits of using the Accused Instrumentalities' compression features, Acronis has injured Realtime and is liable to Realtime for infringement of the '908 patent pursuant to 35 U.S.C. § 271.

51. As a result of Acronis's infringement of the '908 patent, Plaintiff Realtime is entitled to monetary damages in an amount adequate to compensate for Acronis's infringement, but in no event less than a reasonable royalty for the use made of the invention by Acronis, together with interest and costs as fixed by the Court.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 8,717,204

52. Plaintiff realleges and incorporates by reference paragraphs 1-51 above, as if fully set forth herein.

53. Plaintiff Realtime is the owner by assignment of United States Patent No. 8,717,204 entitled "Methods for encoding and decoding data." The '204 patent was duly and legally issued by the United States Patent and Trademark Office on May 6, 2014. A true and correct copy of the '204 Patent is included as Exhibit D.

54. On information and belief, Acronis has offered for sale, sold and/or imported into the United States Acronis products that infringe the '204 patent, and continues to do so. By way of illustrative example, these infringing products include, without limitation, Acronis's products and services, e.g., Acronis Backup Advanced, including version 11.7 thereof, and all versions and variations thereof since the issuance of the '204 patent ("Accused Instrumentality").

55. On information and belief, Acronis has directly infringed and continues to infringe the '204 patent, for example, through its own use and testing of the accused products to practice compression methods claimed by the '204 patent, including a method for processing data, the data residing in data fields, comprising: recognizing any characteristic, attribute, or parameter of the data; selecting an encoder associated with the recognized characteristic, attribute, or parameter of the data; compressing the data with the selected encoder utilizing at

least one state machine to provide compressed data having a compression ratio of over 4:1; and point-to-point transmitting the compressed data to a client; wherein the compressing and the transmitting occur over a period of time which is less than a time to transmit the data in an uncompressed form. On information and belief, Acronis uses the Accused Instrumentality in its ordinary and customary fashion for its own internal non-testing business purposes, while testing the Accused Instrumentality, and while providing technical support and repair services for the Accused Instrumentality to Acronis's customers, and use of the Accused Instrumentality in its ordinary and customary fashion results in infringement of the methods claimed by the '204 patent.

56. On information and belief, Acronis has had knowledge of the '204 patent since at least the filing of this Complaint or shortly thereafter, and on information and belief, Acronis knew of the '204 patent and knew of its infringement, including by way of this lawsuit.

57. Acronis's affirmative acts of making, using, selling, offering for sale, and/or importing the Accused Instrumentality have induced and continue to induce users of the Accused Instrumentality to use the Accused Instrumentality in its normal and customary way to infringe the '204 patent by practicing compression methods claimed by the '204 patent, including a method for processing data, the data residing in data fields, comprising: recognizing any characteristic, attribute, or parameter of the data; selecting an encoder associated with the recognized characteristic, attribute, or parameter of the data; compressing the data with the selected encoder utilizing at least one state machine to provide compressed data having a compression ratio of over 4:1; and point-to-point transmitting the compressed data to a client; wherein the compressing and the transmitting occur over a period of time which is less than a time to transmit the data in an uncompressed form. For example, Acronis explains to customers the benefits of using the Accused Instrumentality: "One of the key capabilities of the Acronis storage node is deduplication. Deduplication technology helps reduce storage costs and network bandwidth utilization by eliminating duplicate data blocks when you back up and transfer data. Acronis Backup Advanced deduplication helps you to: 1. Reduce storage space usage by storing

only unique data 2. Eliminate the need to invest in data deduplication-specific hardware 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks." See http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2. Acronis specifically intended and was aware that the normal and customary use of the Accused Instrumentality on compatible systems would infringe the '204 patent. Acronis performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '204 patent and with the knowledge, or willful blindness to the probability, that the induced acts would constitute infringement. On information and belief, Acronis engaged in such inducement to promote the sales of the Accused Instrumentality, *e.g.,* through Acronis's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '204 patent. Accordingly, Acronis 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 '204 patent, knowing that such use of the Accused Instrumentality with compatible systems will result in infringement of the '204 patent.

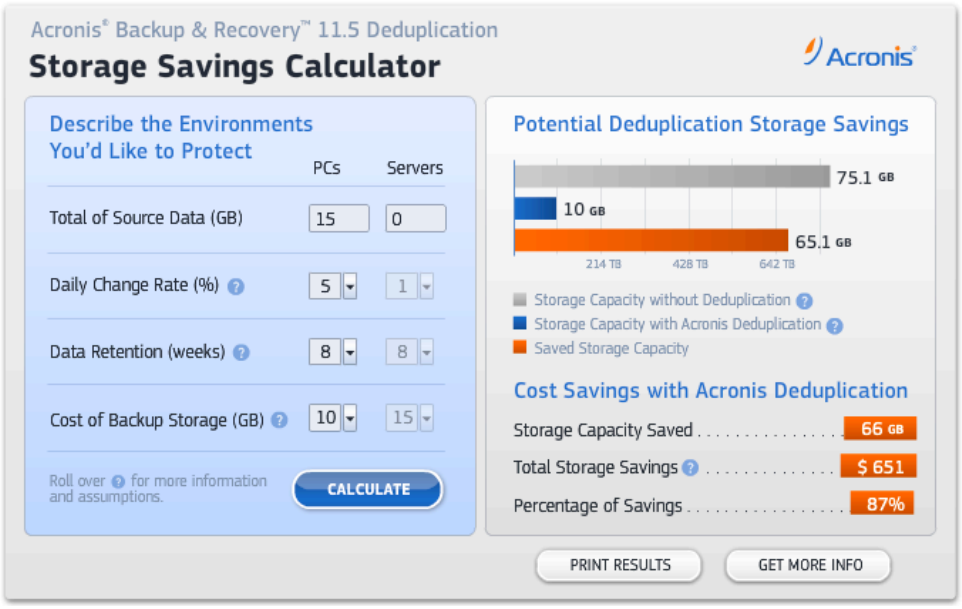
58. The Accused Instrumentality practices a method for processing data, the data residing in data fields. See http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself.").

59. The Accused Instrumentality recognizes any characteristic, attribute, or parameter of the data. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself.").

60. The Accused Instrumentality selects an encoder associated with the recognized characteristic, attribute, or parameter of the data. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("When performing a backup to a deduplicating vault, the Acronis Backup agent calculates a fingerprint or a checksum of each data block. This fingerprint or checksum is often called a hash value. The data block size varies from 1 byte to 256KB for disk-level and file-level backups. Each file that is less than 256KB is considered a complete data block. Files larger than 256KB are split into 256KB blocks. Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself.").

61. Upon information and belief, the Accused Instrumentality compresses the data with the selected encoder utilizing at least one state machine to provide compressed data having a compression ratio of over 4:1. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 20 ("**Compression Ratio**: The data in all types of backups is usually compressed. Default, "normal" compression levels reach from 40 to 60 percent, meaning that the compressed data is 40 to 60 percent of the original data. … **Unique Data Percentage:** The amount of unique data

on a machine depends on the role of the system. The "percent unique" numbers below are derived from Acronis' experience with its customers and may vary in your environment. 1. Virtual machines: 30 percent unique 2. Office workstations: 50 percent unique 3. Database servers: 65 percent unique 4. File servers: 75 percent unique."). For example, Acronis touts that, using deduplication, which is a form of compression, "[a] reasonable expectation for typical environments with 20-30 machines is a ratio of between 10% and 3% (provided the average amount of unique data in total is approximately 10% and also using full backups instead of incremental/differentials)" indicating compression or space savings of 90% to 97%. *See, e.g.,* https://kb.acronis.com/content/37089. Acronis further states "[r]eduction of data up to 90% with deduplication and compression." *See, e.g.,* http://dl2.acronis.com/u/pdf/BackupRecoveryDeduplication_datasheet.en_eu.pdf ("it is possible to achieve, using data deduplication, compression ratios of 1:20 or higher."); *see also, e.g.,* https://kb.acronis.com/content/56205 ("Compression ratio: 1:4"); https://www.mirrorsphere.com/acronis-universal-backup/ ("Compression ratio: 1:6"). Acronis's deduplication ROI calculator also yields compression ratio of over 4:1. *See, e.g.,* https://www.acronis.com/en-us/backup-recovery/deduplication-roi-calculator.html. The foregoing example evidence indicates that the Accused Instrumentality compresses the data with the selected encoder utilizing at least one state machine to provide compressed data having a compression ratio of over 4:1.



62. The Accused Instrumentality point-to-point transmits the compressed data to a client. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 5 ("Before sending the data block to the vault, the agent queries the storage node to determine whether the block's hash value is already stored there. If so, the agent sends only the hash value; otherwise, it sends the block itself. The storage node saves the received data blocks in a temporary file.").

63. In the Accused Instrumentality, the compressing and the transmitting occur over a period of time which is less than a time to transmit the data in an uncompressed form. *See, e.g.*, http://dl2.acronis.com/u/pdf/AcronisBackupDeduplication_technical_whitepaper_en-US.pdf at 2 ("Deduplication technology helps reduce storage costs and network bandwidth utilization by eliminating duplicate data blocks when you back up and transfer data. … Acronis Backup Advanced deduplication helps you to: … 3. Reduce network load because less data is transferred, leaving more bandwidth for your production tasks.").

64. On information and belief, Acronis also infringes, directly and through induced infringement, and continues to infringe other claims of the '204 patent, for similar reasons as explained above with respect to Claim 12 of the '204 patent.

65. By making, using, offering for sale, selling and/or importing into the United States the Accused Instrumentalities, and touting the benefits of using the Accused Instrumentalities' compression features, Acronis has injured Realtime and is liable to Realtime for infringement of the '204 patent pursuant to 35 U.S.C. § 271.

66. As a result of Acronis's infringement of the '204 patent, Plaintiff Realtime is entitled to monetary damages in an amount adequate to compensate for Acronis's infringement, but in no event less than a reasonable royalty for the use made of the invention by Acronis, together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Realtime respectfully requests that this Court enter:

a. A judgment in favor of Plaintiff that Acronis has infringed, either literally and/or under the doctrine of equivalents, the '728 patent, the '530 patent, the '908 patent, and the '204 patent;

b. A permanent injunction prohibiting Acronis from further acts of infringement of the '728 patent, the '530 patent, the '908 patent, and the '204 patent;

c. A judgment and order requiring Acronis to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for its infringement of the '728 patent, the '530 patent, the '908 patent, and the '204 patent; and

d. A judgment and order requiring Acronis to provide an accounting and to pay supplemental damages to Realtime, 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 Defendants; 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: September 22, 2017

Respectfully submitted,

PLAINTIFF REALTIME DATA LLC d/b/a IXO,
By its attorneys,

/s/ Marc A. Fenster

Marc A. Fenster (CA SBN 181067)
Reza Mirzaie (CA SBN 246953)
Brian D. Ledahl (CA SBN 186579)
C. Jay Chung (CA SBN 252794)
RUSS AUGUST & KABAT
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
Tel: (310) 826-7474
mfenster@raklaw.com
rmirzaie@raklaw.com
bledahl@raklaw.com
jchung@raklaw.com

David S. Godkin (BBO#196530)
James E. Kruzer (BBO#670827)
BIRNBAUM & GODKIN, LLP
280 Summer Street, 5th Fl.
Boston, MA, 022110
Tel: (617) 307-6100
Fax: (617) 307-6101
godkin@birnbaumgodkin.com
kruzer@birnbaumgodkin.com

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the above document was served on September 22, 2017 upon the counsel of record who are deemed to have consented to electronic service via the Court's CM/ECF system per Local Rule 5.2(b). Any other counsel of record will be served by electronic mail or first class mail on this same date.

/s/ Marc A. Fenster