

**Before the
Federal Trade Commission
Washington, DC 20580**

In the Matter of)
)
Dropbox, Inc.)

May 11, 2011

**REQUEST FOR INVESTIGATION AND
COMPLAINT FOR INJUNCTIVE RELIEF**

SUMMARY

1. Dropbox has prominently advertised the security of its “cloud” backup, sync and file sharing service, which is now used by more than 25 million consumers, many of whom “rely on Dropbox to take care of their most important information.”¹
2. Dropbox does not employ industry best practices regarding the use of encryption technology. Specifically, Dropbox’s employees have the ability to access its customers’ unencrypted files.
3. Dropbox has and continues to make deceptive statements to consumers regarding the extent to which it protects and encrypts their data.
4. Dropbox’s customers face an increased risk of data breach and identity theft because their data is not encrypted according to industry best practices.
5. If Dropbox disclosed the full details regarding its data security practices, some of its customers might switch to competing cloud based services that do deploy industry best practices regarding encryption, protect their own data with 3rd party encryption tools, or decide against cloud based backups completely.
6. Dropbox’s misrepresentations are a Deceptive Trade Practice, subject to review by the Federal Trade Commission (the “Commission”) under section 5 of The Federal Trade Commission Act.

¹ Drew Houston and Arash Ferdowsi, Privacy, Security & Your Dropbox, The Dropbox Blog, April 21, 2011, available at <http://blog.dropbox.com/?p=735>

PARTIES

7. Christopher Soghoian is a Washington, D.C. based Graduate Fellow at the Center for Applied Cybersecurity Research at Indiana University, and a Ph.D. Candidate in the School of Informatics and Computing at Indiana University. His research is focused at the intersection of security, privacy, law and policy. This complaint is submitted in his personal capacity.
8. Dropbox, Inc. ("Dropbox") was founded in 2007 and is based in San Francisco, California. Dropbox's headquarters are located at 760 Market Street #1150, San Francisco, CA 94102. At all times material to this complaint, Dropbox's course of business, including the acts and practices alleged herein, has been and is in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 45.

STATEMENT OF FACTS

9. Dropbox is a file backup, synchronization and sharing service enabling users to store their photos, documents and other files "in the cloud."
10. Dropbox's software automatically backs up files from user-specified directories onto the company's servers. These files and folders can be synchronized between multiple computers and shared with other users.
11. As of April 2011, Dropbox is reported to have 25 million users and 200 million files are "saved" using the service each day.²
12. Dropbox provides 2GB of storage space to its customers for free. Consumers can purchase additional storage space, by signing up for one of two "Pro" service plans, offering 50GB for \$9.99/month or \$99.00/year, and 100GB for \$19.99/month or \$199.00/year.³

DROPBOX PROMINENTLY ADVERTISES THE SECURITY AND SAFETY OF ITS SERVICE

13. On the "install" page on the Dropbox website, visitors are told that "Your files are always safe."⁴

² Michael Arrington, Dropbox Hits 25 Millions Users, 200 Million Files Per Day, TechCrunch, April 17, 2011, available at <http://techcrunch.com/2011/04/17/dropbox-hits-25-millions-users-200-million-files-per-day/>.

³ <https://www.dropbox.com/plans>

⁴ <https://www.dropbox.com/install>

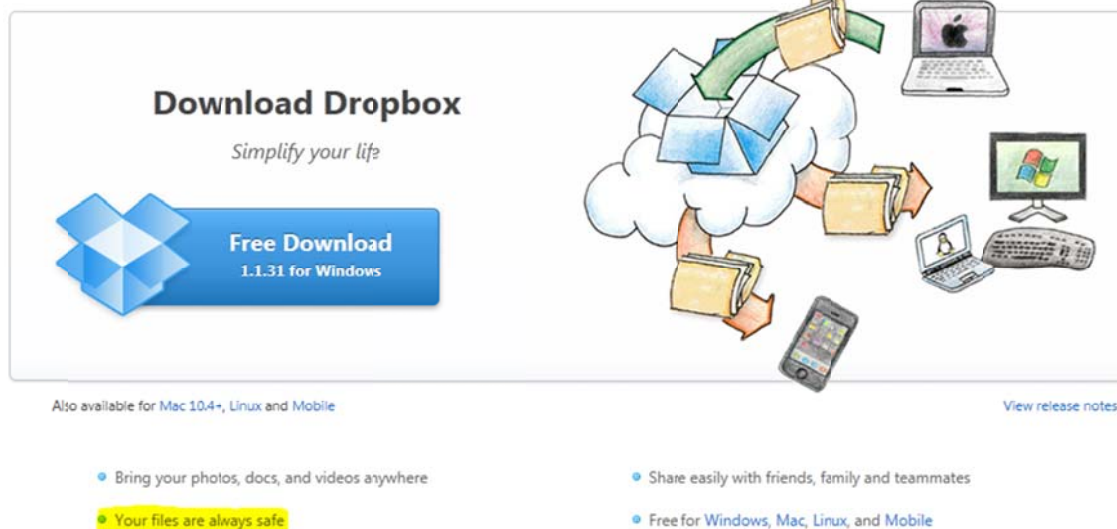


Figure 1: The "Install" page on Dropbox's website.

14. On the "product features" page on the Dropbox site, visitors are told that their files are safe, and that the company uses encryption to protect the files stored on Dropbox's servers.⁵

Your stuff is safe

Dropbox protects your files without you needing to think about it.

- Dropbox keeps a one-month history of your work.
- Any changes can be undone, and files can be undeleted.
- All transmission of file data occurs over an encrypted channel (SSL).
- All files stored on Dropbox are encrypted (AES-256).

Figure 2: The "Product Features" page on Dropbox's website.

15. Until April 13, 2011, the "How Secure is Dropbox" page in the "Help Center" section of Dropbox's website included the following specific claims regarding the security of users' data:⁶

"All files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without your account password."

⁵ <https://www.dropbox.com/features>

⁶ This page has been changed at least twice since April 12, 2011. The latest version can be accessed at <https://www.dropbox.com/help/27>.

“Nobody can see your private files in Dropbox unless you deliberately invite them or put them in your Public folder.”

“Dropbox employees aren’t able to access user files, and when troubleshooting an account they only have access to file metadata (filenames, file sizes, etc, not the file contents).”

“Your files are actually safer while stored in your Dropbox than on your computer in some cases. We use the same secure methods as banks and the military to send and store your data.”

How secure is Dropbox?

Your files are actually safer while stored in your Dropbox than on your computer in some cases. We use the same secure methods as banks and the military to send and store your data.

Dropbox takes the security of your files and of our software very seriously. We use the best tools and engineering practices available to build our software, and we have smart people making sure that Dropbox remains secure. Your files are backed-up, stored securely, and password-protected.

Nobody can see your private files in Dropbox unless you deliberately [invite them](#) or put them in your Public folder. Everything in your Public folder is, by definition, [accessible to anyone](#). Otherwise, the only way to access the files in your Dropbox online is with your username and password.

For Our Advanced Users

Dropbox uses modern encryption methods to both transfer and store your data.

- Shared folders are viewable only by people you invite
- All transmission of file data occurs over an encrypted channel (SSL).
- All files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without your account password
- Dropbox website and client software have been hardened against attacks from hackers
- Online access to your files requires your username and password
- Public files are only viewable by people who have a link to the file(s). Public folders are not browsable or searchable
- Dropbox employees aren't able to access user files, and when troubleshooting an account they only have access to file metadata (filenames, file sizes, etc., not the file contents)

Dropbox uses Amazon's Simple Storage Service (S3) for storage, which has a robust security policy of its own. You can find more information on Amazon's data security from the [S3 site](#) or, read more about [how Dropbox and Amazon securely stores data](#).

Figure 3: The “How Secure is Dropbox” page in the “Help Center” section of Dropbox’s website prior to April 13, 2011.

DROPBOX'S SERVICE DOES NOT PROVIDE STRONG SECURITY

16. The Advanced Encryption Standard (AES) was announced by National Institute of Standards and Technology (NIST) after a 5-year standardization process in which fifteen competing designs were presented and evaluated.⁷
17. The AES standard is comprised of three different encryption ciphers (AES-128, AES-192, AES-256), with key sizes of 128, 192 and 256 bits, respectively.
18. AES is the first publicly accessible and open cipher approved by the National Security Agency (NSA) for top secret information (when the 192 or 256 bit key lengths are used).⁸
19. Dropbox uses AES-256, the highest strength of the AES ciphers to encrypt user data on its servers.⁹ With regard to its choice of encryption algorithm for stored user data, Dropbox follows industry best practices and does indeed “use the same secure methods as banks and the military.”¹⁰
20. The choice of encryption algorithms is an important component in the security of a system. However, equally important is the storage and management of the keys used to encrypt data.
21. The keys used to encrypt users’ data are known to some Dropbox employees and stored on the company’s servers.¹¹
22. Dropbox’s use and storage of encryption keys does not follow best practices for the “cloud” backup industry.¹² Several competing services, such as

⁷ See generally:

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process

⁸ Lynn Hathaway, "National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information", June 2003, available at

<http://csrc.nist.gov/groups/ST/toolkit/documents/aes/CNSS15FS.pdf>

⁹ “How Secure is Dropbox” available at <https://www.dropbox.com/help/27>

¹⁰ *Id.*

¹¹ Post by “N.N”, Dropbox employee, in Dropbox support forum,

<http://forums.dropbox.com/topic.php?id=3908#post-27169> (“Currently there is only one key, that the DB team has. Not the most ideal situation, granted, but there has been discussion about enabling private keys for people. (Note that this will break the “quick upload” feature for files not already in your account.)”)

¹² The Open Web Application Security Project (OWASP), Guide to Cryptography, available at https://www.owasp.org/index.php/Guide_to_Cryptography (“The strength of a cryptographic system is measured in key length. Using a large key

SpiderOak¹³ and Wuala,¹⁴ encrypt users' data, by default, with a key only known to each user. These competing companies do not have the ability to access their customers' unencrypted data.

23. Responding to a query from a customer on the official support forum regarding the encryption keys and security of Dropbox's architecture, Arash Ferdowsi, the company's CTO revealed that:

"The only 100% safe option with any online storage solution is (as you said) to encrypt on your own. [M]any dropbox users use truecrypt with no problems :-)." ¹⁵

24. Although Mr Ferdowsi has acknowledged in the support forum that his company's service is not "100% safe,"¹⁶ the company prominently advertises to consumers that "[y]our files are always safe" when stored with the service.¹⁷

25. On April 1, 2011, Marcia Hofmann of the Electronic Frontier Foundation contacted Dropbox on my behalf.¹⁸ Among the suggestions we made to the company were the following:

- a. Update the statements made on its website to disclose details regarding the company's use of encryption, and the fact that it has the ability to access users' data.
- b. Notify its customers by email to let them know that the service is not in fact encrypting their data with a key only known to the user.
- c. Switch to a model of encrypting user data with a key only known to the user.

length and then storing the unprotected keys on the same server eliminates most of the protection benefit gained.")

¹³ Nuts and Bolts, Spideroak, available at

https://spideroak.com/engineering_matters.

¹⁴ Security and Privacy, FAQ, Wuala, available at

<http://www.wuala.com/en/support/faq/c/20>; Security, Wuala, available at

<http://www.wuala.com/en/learn/technology>.

¹⁵ Arash F., Post to Support forum thread "Files: Encrypted or not?",

<http://forums.dropbox.com/topic.php?id=17666#post-109672>

¹⁶ *Id.*

¹⁷ Dropbox install page, <https://www.dropbox.com/install>.

¹⁸ Email from Marcia Hofmann to Arash Ferdowsi, April 1, 2011.

26. On April 12th, 2011, I published a post to my blog highlighting privacy problems associated with Dropbox's service.¹⁹ Soon after, prominent bloggers and members of the technology press wrote about the topic.²⁰

DISCLOSURES BY DROPBOX SINCE APRIL 13th, 2011 ARE INSUFFICIENT

27. In response to Marcia Hofmann's email, my blog post, and the subsequent press attention, Dropbox modified several statements made on their website.

28. On or around April 14th, 2011, one of the statements on the "How Secure is Dropbox" page in the "Help Center" section of Dropbox's website was changed from "All files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without your account password" to "All files stored on Dropbox servers are encrypted (AES-256)."

29. On April 23, 2011, the "How Secure is Dropbox" page was again modified.

- a. The following statement was removed entirely: "Online access to your files requires your username and password."
- b. The statement "Nobody can see your private files in Dropbox unless you deliberately invite them or put them in your Public folder" was modified to be "Other Dropbox users can't see your private files in Dropbox unless you deliberately invite them or put them in your Public folder."
- c. The statement "Dropbox employees aren't able to access user files, and when troubleshooting an account they only have access to file

¹⁹ Christopher Soghoian, How Dropbox sacrifices user privacy for cost savings , Slight Paranoia, April 12, 2011, available at <http://paranoia.dubfire.net/2011/04/how-dropbox-sacrifices-user-privacy-for.html>

²⁰ Cory Doctorow, Dropbox's new security policy implies that they lied about privacy from the start - UPDATED, BoingBoing, April 21, 2011, available at <http://boingboing.net/2011/04/21/dropboxs-new-securit.html>; Miguel de Icaza, Dropbox Lack of Security, Personal Blog, April 19, 2011, available at <http://tirania.org/blog/archive/2011/Apr-19.html>; Klint Finley, How to Keep Dropbox Employees' Hands Off Your Data , ReadWrite Cloud, April 20, 2011, available at <http://www.readwriteweb.com/cloud/2011/04/how-to-keep-dropbox-employees.php>; Erik Sherman, "At Dropbox, Even We Can't See Your Data - Er, Nevermind" [Update], BNET, available at <http://www.bnet.com/blog/technology-business/-8220at-dropbox-even-we-can-8217t-see-your-dat-8211-er-nevermind-8221-update/10077>.

metadata (filenames, file sizes, etc, not the file contents)” was modified to read “Dropbox employees are prohibited from viewing the content of files you store in your Dropbox account, and are only permitted to view file metadata (e.g., file names and locations).”

d. A new statement was also added to the page:

“Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that’s the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.”

30. Although the company has added some clarifying disclosures to its website, the firm continues to make unqualified claims regarding the safety and security of its service on the “Features” and “Install” pages on its site, both of which are linked to from the homepage, and far more likely to be viewed by the average user than the website’s “Help Center”.

31. Dropbox has not contacted its 25 million existing customers to let them know about the changes to its privacy policy, or the fact that the company does in fact have access to their unencrypted data.

DROPBOX HAS MISLEAD ITS CUSTOMERS REGARDING THE EXTENT TO WHICH THEIR DATA IS PROTECTED

32. On April 21, 2011, Dropbox’s CTO and CEO published a post to company’s official blog regarding the extent to which the company has access to user data.²¹

33. Comments left at the bottom of that blog post and in the company’s support forum make it clear that some of Dropbox’s customers (including “Pro” users who have paid for the service) were upset, and felt that the company had lied to them.²²

²¹ Drew Houston and Arash Ferdowsi, Privacy, Security & Your Dropbox, The Dropbox Blog, April 21, 2011, available at <http://blog.dropbox.com/?p=735>

²² Comment by Brent C., available at <http://forums.dropbox.com/topic.php?id=36814#post-312492>; Comment by Joshua P., available at

★ Brent C.
Pro User
Posts: 1

I am thinking of going back to free. This dichotomy has yet to be explained to me by Dropbox Staff. They either do have access to my data (and I'm out) or they don't (in which case giving the data to the Government means nothing as no one can crack AES-256 yet without the key, therefore what's the point in changing their TOS).

I feel scammed.

★ Joshua P.
Pro User
Posts: 15

Arash F., why not just say that Dropbox's marketing was a flat out lie?

I signed up with the service being told that Dropbox employees CAN NOT access my data, but instead it's really they MAY NOT access the data. That's a huge difference.



Xyzy 1 week ago in reply to krisu

So what? I signed up for DropBox and paid for a one-year subscription based on that assurance -- that everything was transmitted and stored in an encrypted format, and DropBox itself had no technological way of decrypting that information.

There's no other way of interpreting that statement. That statement means that DropBox does not store the decryption keys. I reasonably believed, based on that statement, that all data was encrypted before it left my computer, and couldn't be decrypted except on my computer. I.e., like a cloud-based version of TrueCrypt.

Now they're telling us "actually, we do store your keys, in case that we need to decrypt your data." I'll take them at their word that the keys are stored in a safe manner, and that this is rarely done. However, their original statement was a lie. Moreover, the fact that they store the encryption keys automatically creates a security vulnerability -- no matter how secure they might think their key-storage system is, nothing's perfect.

Perhaps this security isn't as important for you. However, that doesn't mean that it isn't important for other people.



Justin Cardinal 1 week ago in reply to Kemp

FWIW, I considered creating a TrueCrypt volume to store sensitive data within my Dropbox account. After reading their information that said the information was encrypted and that their own employees couldn't access it, I made a conscious decision that the extra layer was unnecessary because the data was already secure. That's the problem; people made decisions about the security of their data based on what Dropbox claimed, and now it turns out those claims were untrue.

34. On April 19th, 2011, Jon Callas, the co-founder and former CTO of Pretty Good Privacy (PGP) posted the following message to his public Twitter account:²³

<http://forums.dropbox.com/topic.php?id=36835&replies=33#post-312775>;
Comment by Xyzy, available at <http://blog.dropbox.com/?p=735#comment-189261869>; Comment by Justin Cardinal, available at <http://blog.dropbox.com/?p=735#comment-190051017>

²³ <https://twitter.com/#!/joncallas/status/60401887140261888>



@joncallas
Jon Callas

I deleted my Dropbox account. It turns out that they lied and don't actually encrypt your files and will hand them over to anyone who asks.

19 Apr via web ☆ Favorite ↻ Undo Retweet ↩ Reply

35. If a prominent cryptographer and security expert was misled by Dropbox's statements regarding its use of encryption, it seems entirely unreasonable to expect that the average non-technical user would have been able to read between the lines and determine that the company was not in fact using encryption with a key only known to the user.
36. Several members of the technology press were also misled by Dropbox's claims.

- a. Richard Gaywood at The Unofficial Apple Weblog writes that:

"AES-256 is a very secure encryption scheme which basically makes it impossible to hack into the encrypted files without the decryption key. Dropbox's FAQ copy makes it sound like its employees don't have access to this key -- as though it's generated from your Dropbox password, perhaps. That's certainly what I took away from the Dropbox FAQ."²⁴

- b. Robert Vamosi at PC World wrote that:

"Storing data via the cloud solves problems, enabling you to access your files from a remote location. But it also creates frightening scenarios of other, unauthorized people accessing your personal data. One way to mitigate that risk is to choose cloud services that include data encryption.

For example, the Dropbox remote-file-storage site employs a full-encryption Secure Sockets Layer (SSL) protocol when you

²⁴ Richard Gaywood, Dropbox under fire for security concerns (updated), The Unofficial Apple Weblog, April 19, 2011, available at <http://www.tuaw.com/2011/04/19/dropbox-under-fire-for-security-concerns/>

upload a file, and uses strong AES 256 encryption for the data you store within the cloud.”²⁵

DROPBOX’S USE OF A COMMON ENCRYPTION KEY KNOWN TO THE COMPANY UNNECESSARILY EXPOSES ITS CUSTOMERS TO RISK

37. In their April 21, 2011 blog post, Dropbox’s CEO and CTO have acknowledged that some of their employees have the ability to access users’ unencrypted data:

“Like most major online services, we have a small number of employees who must be able to access user data when legally required to do so. But that’s the exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances.”²⁶

38. “Insider” attacks are a major source of privacy violations and data breaches. Employees at Google,²⁷ Facebook,²⁸ the State Department,²⁹ and Kaiser Permanente³⁰ have all reportedly accessed the private files of customers.

39. Although Dropbox’s policies prohibit its employees from accessing users’ unencrypted data except when legally compelled to do so,³¹ similar policies likely existed at Google, Facebook and Kaiser Permanente.

40. In addition to the threat of rogue employees, Dropbox has exposed its users to unnecessary risk of data theft by hackers who, if they break into the

²⁵ Robert Vamosi, Protect Your Online Privacy (Without Reading All the Fine Print), PCWorld, March 30, 2011, available at http://www.pcworld.com/businesscenter/article/221104/protect_your_online_privacy_without_reading_all_the_fine_print.html

²⁶ Drew Houston and Arash Ferdowsi, Privacy, Security & Your Dropbox, The Dropbox Blog, April 21, 2011, available at <http://blog.dropbox.com/?p=735>

²⁷ Adrian Chen, GCreep: Google Engineer Stalked Teens, Spied on Chats (Updated), Gawker, September 14, 2010, available at <http://gawker.com/#!5637234>

²⁸ Ryan Tate, Why You Shouldn’t Trust Facebook with Your Data: An Employee’s Revelations, Gawker, January 11, 2010, available at <http://gawker.com/#!5445592/why-you-shouldnt-trust-facebook-with-your-data-an-employees-revelations>

²⁹ Passport files of candidates breached, Associated Press, March 21, 2008, available at <http://www.msnbc.msn.com/id/23736254/>

³⁰ Kaiser Permanente Bellflower Medical Center, Associated Press, March 31, 2009, available at <http://www.foxnews.com/story/0,2933,511721,00.html>

³¹ Drew Houston and Arash Ferdowsi, Privacy, Security & Your Dropbox, The Dropbox Blog, April 21, 2011, available at <http://blog.dropbox.com/?p=735>

company's servers, may be able to steal users' data and the keys necessary for decryption.

41. Recent high profile data breaches experienced by RSA,³² Comodo,³³ and Lastpass³⁴ demonstrate that hackers are increasingly sophisticated, and are now seeking out high-value infrastructure targets that can deliver more than just a few million credit card numbers.
42. If Dropbox encrypted its users' data with a key only known to each user, it would not be possible for rogue employees to snoop on users' data, or for hackers who had broken into the company's servers to get access to user' unencrypted data.

DROPBOX'S MISLEADING STATEMENTS ABOUT ENCRYPTION GIVE IT AN UNFAIR ADVANTAGE OVER COMPETING CLOUD BACKUP SERVICES THAT DO PROTECT THEIR CUSTOMER'S DATA

43. Several of Dropbox's competitors do in fact encrypt user data with a key only known to that user. These firms pay higher bandwidth and storage costs than Dropbox, as they do not deduplicate data across user accounts.³⁵
44. Dropbox and its competitors all mention their use of "encryption" when marketing the security of their products. Especially prior to April 2011, the average, non-technical consumer would have no way of knowing that

³² John Markoff, SecurID Company Suffers a Breach of Data Security, The New York Times, March 17, 2011, available at

<https://www.nytimes.com/2011/03/18/technology/18secure.html>

³³ Riva Richmond, An Attack Sheds Light on Internet Security Holes, The New York Times, April 6, 2011, available at

<https://www.nytimes.com/2011/04/07/technology/07hack.html>

³⁴ Amy Gahran, Password-storing service may have been hacked, CNN, May 5, 2011, available at <http://www.cnn.com/2011/TECH/web/05/05/last.pass.gahran/>

³⁵ Danny Harnik, Benny Pinkas and Alexandra Shulman-Peleg Side Channels in Cloud Services, the Case of Deduplication in Cloud Storage IEEE Security and Privacy Magazine, special issue of Cloud Security, Vol. 8, No. 2, pp. 40-47, 2010. ("By storing and transmitting only a single copy of duplicate data, deduplication saves both disk space and network bandwidth. For vendors [like Dropbox], it offers secondary cost savings in power and cooling achieved by reducing the number of disk spindles."); See also, Alan Fairless, Why SpiderOak doesn't de-duplicate data across users (and why it should worry you if we did), Spideroak Blog, August 27, 2010, available at <https://spideroak.com/blog/20100827150530-why-spideroak-doesnt-de-duplicate-data-across-users-and-why-it-should-worry-you-if-we-did>

Dropbox's use of AES-256 encryption is significantly inferior to that of its competitors.

45. These other firms are unfairly placed at a competitive disadvantage. Dropbox uses the same terminology to market the security of its products, but has lower operating costs, due to its inferior security.
46. If the Commission wishes for companies to embrace Privacy by Design,³⁶ it must guarantee that those firms that pay a cost for doing so are able to effectively compete in the market.

**THIS IS NOT AN ISOLATED ISSUE: DROPBOX HAS ALSO DECEIVED ITS
USERS REGARDING THE SECURITY OF ITS MOBILE CLIENT**

47. Until mid-March, 2011, the "How Secure is Dropbox" page in the "Help Center" section of Dropbox's website page included the following statement:

"All transmission of file data and metadata occurs over an encrypted channel (SSL)."

48. Contrary to these unqualified claims, the company is in fact not using SSL encryption to transmit all file data and metadata. On March 10, 2011, technologist Mike Cardwell revealed that Dropbox's Android mobile client is not using SSL to transmit file metadata to Dropbox's servers.³⁷
49. When Mr. Cardwell contacted Dropbox's support team to ask about the validity of the claim on the company's website, he was told that:

"The information in the help center is in relation to the Dropbox desktop and website and doesn't apply to the mobile interface. I'm sorry that this isn't more clearly defined. I will discuss this further with our mobile team to see if we can offer the option of total transmission encryption on the phone and update this document to reflect the current status of metadata transmission."

³⁶ See generally, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Consumers, Preliminary FTC Staff Report, December 2, 2010, available at <http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>

³⁷ Mike Cardwell, Dropbox Mobile: Less Secure Than Dropbox Desktop, Post to Grepular Blog, March 10, 2011, available at https://grepular.com/Dropbox_Mobile_Less_Secure_Than_Dropbox_Desktop

50. The April 2011 blog post by Dropbox's CEO and CTO also acknowledged that the company had opted to trade security for performance on the mobile client:

"We made this decision to provide better performance (in our testing, enabling SSL for all metadata transfers made the app several times slower). We've listened to these concerns, and are working on a faster way to transmit metadata over SSL on the mobile apps."

DROPBOX'S STATEMENTS ABOUT ENCRYPTION ARE A DECEPTIVE BUSINESS PRACTICE

51. According to the FTC Policy Statement on Deception,³⁸ there are three elements to any deception case.

- a. There must be a representation, omission or practice that is likely to mislead the consumer.
- b. The practice must be deceptive from the perspective of the average consumer.
- c. The representation, omission, or practice must be a "material" one, and thus whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service.

52. As documented earlier in this complaint, the "How Secure is Dropbox" page in the "Help Center" section on Dropbox's website included several misleading statements until the page was modified in April, 2011. These included:

- a. "All files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without your account password."
- b. "Nobody can see your private files in Dropbox unless you deliberately invite them or put them in your Public folder."
- c. "Dropbox employees aren't able to access user files, and when troubleshooting an account they only have access to file metadata (filenames, file sizes, etc, not the file contents)."

³⁸ FTC Policy Statement on Deception, October 14, 1983, available at <http://www.ftc.gov/bcp/policystmt/ad-decept.htm>

- d. "Your files are actually safer while stored in your Dropbox than on your computer in some cases."
53. The company continues to mislead consumers on the "Install" and "Features" pages on its website. By telling consumers that their data is "always safe," and that the data is encrypted with AES-256 without informing them that the company has access to the key used to decrypt it, the company is omitting a material fact regarding the degree of security and privacy delivered by the service.
54. Had Dropbox not made these deceptive statements, its customers might have opted to protect their data by using a competing cloud based backup service that encrypts their data with a key only known to them, by using 3rd party encryption tools, or opting to not store their sensitive data in the cloud at all.

REQUEST FOR RELIEF

I request that the Commission investigate Dropbox and enjoin its deceptive business practices. Specifically, I request that the Commission:

- a. Compel Dropbox to clarify existing statements on the "Install" and "Features" sections of its website to note that the company does in fact have access to users' unencrypted data and that a data breach of the company's servers could lead to the theft of users' unencrypted data.
- b. Compel Dropbox to contact its 25 million existing customers by email to notify them that it has access to their unencrypted data and to suggest specific steps they can take to secure it (such as by using 3rd party encryption software).
- c. Compel Dropbox to offer refunds to anyone that has purchased its "Pro" service that felt misled by the company's statements regarding security.
- d. Prohibit Dropbox from making deceptive statements in the future regarding the privacy and security of its services.

I reserve the right to supplement this petition as other information relevant to this proceeding becomes available.

Respectfully submitted,

/s/

Christopher Soghoian