David C. Parisi, Esq. (162248)
dparisi@parisihavens.com
Suzanne Havens Beckman (188814)
shavens@parisihavens.com
PARISI & HAVENS LLP
15233 Valleyheart Drive
Sherman Oaks, CA 91403
Telephone: (818) 990-1299

Joseph H. Malley (not admitted)
malleylaw@gmail.com
LAW OFFICE OF JOSEPH H. MALLEY
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

Alan Himmelfarb (90480)
THE LAW OFFICES OF ALAN HIMMELFARB
80 W. Sierra Madre Blvd., # 304
Sierra Madre, CA 91024
Telephone: (626) 325-3104
consumerlaw1@earthlink.net

Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

FRANCISCO ESPITIA, VANESSA ZENDEJAS, and JOE A. SANCHEZ FRAIRE, individually and on behalf of a class of similarly situated individuals, Plaintiffs, v. HIPSTER, INC., a Delaware Corporation; Defendant.	CASE No. JURY DEMAND COMPLAINT FOR: 1. Electronic Communications Privacy Act, 18 U.S.C. §2510; 2. Stored Communications Act, 18 U.S.C. § 2701; 3. California Computer Crime Law, Penal Code § 502; 4. California's Invasion Of Privacy Act, California Penal Code § 630; 5. California Unfair Competition Law, Business and Professions Code § 17200; 6. Bailment;

7. Conversion;
8. Invasion of Privacy and Seclusion and Public Disclosure of Private Facts;
9. Negligence;
10. Trespass to Personal Property / Chattels; and
11. Unjust Enrichment

CLASS ACTION COMPLAINT

Plaintiffs, FRANCISCO ESPITIA ("Espitia"), VANESSA ZENDEJAS ("Zendejas"), and JOE A. SANCHEZ FRAIRE ("Fraire"), (hereinafter collectively referred to as "Plaintiffs"), by and through their attorneys Parisi & Havens LLP, the Law Offices of Alan Himmelfarb, and the Law Office of Joseph H. Malley, P.C., bring this action on behalf of themselves and all others similarly situated against Defendant HIPSTER, INC.. Plaintiffs' allegations as to themselves and their own actions, as set forth herein, are based upon their information and belief and personal knowledge, and all other allegations are based upon the investigations of counsel. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d) as set forth below.

I. NATURE OF THE ACTION

1. This consumer Class Action involves the "computer hacking" of mobile devices.

2. Defendant Hipster offered to the public an 'App' (a downloadable computing program designed to provide an enhanced user capability for a mobile device, such as an iPhone, iPad or iPod) (hereinafter "Hipster App"). The Hipster App ostensibly was designed to permit users to create postcards from photos taken on iPhone and Android devices. The postcards become attached to the locations they were sent from so it can be easier to document memories. Users were given the option to share photographic postcards with others through their mobile device.

3. However, when users downloaded the Hipster App onto their mobile devices, the Hipster App engaged in additional activities that were not disclosed to the user.

4. The Hipster App, without seeking to obtain consent, and without notice to the user, sought out and retrieved the list of personal contacts on the user's mobile device. This list

of personal contacts was copied and surreptitiously uploaded to Hipster's third-party servers. In addition to the list of personal contacts of the user, other highly sensitive information such as passwords and geo-location were also obtained by the Hipster App. All of this material was sent unencrypted over publicly accessible data channels.

5. These actions involved the deliberate and intentional circumvention of technical measures within the mobile computing device in order to bypass the technical and code based barriers, including the Plaintiffs' and Class Members' privacy settings which were intended to limit access by anyone other than the owner of the device.

6. Once Defendant transferred the users' contact address data to its remote computing service, Hipster then proceeded to access and use such data without authorization or consent.

7. Plaintiffs bring this consumer class action lawsuit pursuant to Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), on behalf of themselves and a proposed class of similarly situated individuals, (hereinafter collectively referred to as the "Class"), who were victims of Hipster's unfair, deceptive, and unlawful business practices.

8. Hipster individually, and in concert with other Hipster Affiliates, has been systematically engaged in and facilitated a covert operation of surveillance of Class Members and violating one or more of the following:

1) Violations of the Electronic Communications Privacy Act, 18 U.S.C. §2510;
2) Violations of the Stored Communications Act, 18 U.S.C. § 2701;
3) Violations of California Computer Crime Law, Penal Code § 502;
4) Violations of California's Invasion Of Privacy Act, California Penal Code § 630;
5) Violations of California Unfair Competition Law, Business and Professions Code § 17200;
6) Bailment;
7) Conversion;

8) Invasion of Privacy and Seclusion and Public Disclosure of Private Facts;

9) Negligence;

10) Trespass to Personal Property / Chattels; and

11) Unjust Enrichment

II. PARTIES

9. Plaintiff Francisco Espitia ("Espitia") is a resident of Dallas County, Texas.

10. Plaintiff Vanessa Zendejas ("Zendejas") is a resident of Dallas County, Texas.

11. Plaintiff Joe A. Sanchez Fraire ("Fraire") is a resident of Dallas County, Texas.

12. Defendant Hipster, Inc. was a privately held Delaware corporation headquartered at 650 Page Mill Rd, Alto, CA 94304.

13. Hipster operates an internet business as a smartphone-based social network utilizing an application software that performs specific functions for a web-based platform on mobile devices. Launched in January 2011, Hipster is located online at https://hipster.com/ Hipster is located within the Apple iTunes store at: https://itunes.apple.com/us/app/hipster/id461983020?mt=8Hipster and in the Android Market at: http://www.androidtapp.com/hipster/

14. On or around March, 2012, Hipster was acquired by AOL, Inc., a New York Corporation, doing business throughout the State of California and the United States.

III. JURISDICTION AND VENUE

15. This Court has jurisdiction over the subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1331.

16. This Court has jurisdiction over Defendant because it is a corporation headquartered in San Francisco County, California, and is a citizen of the state of California. Plaintiffs assert claims on behalf of a proposed class whose members are domiciled throughout the fifty states and the U.S. territories. There is minimal diversity of citizenship between proposed Class Members and Defendants.

17. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendant is a corporation headquartered in San Francisco County, California, and/or because the improper conduct alleged in this Complaint occurred in, was directed from, and/or emanated from this judicial district.

IV. INTRADISTRICT ASSIGNMENT

18. Pursuant to Local Rule 3-5(b) and 3-2(c), this action should be assigned to the San Francisco Division of the Northern District of California because Defendant resides in San Francisco.

V. FACTUAL BACKGROUND

A. General Overview

19. Hipster describes its business as a method to "Easily share where you are and what you're doing with postcards of your photos."

20. Defendant Hipster's App allows users to upload digital pictures from their mobile devices to create a postcard-like frame around the picture, and a location to show on social network platforms, such as Facebook, Twitter, Flickr, Tumblr or Foursquare. Defendant promoted itself as a way to help people explore a place by glancing through other people's pictures taken nearby and topped with photo filters and frames. The social element to the service let users view posted pictures from various parts of the world and view popular posts locally and globally. Users can select themes, resize the image by cropping, and can also tag friends in the picture itself. However, without adequate notice to users, all content was public by default, so that each upload contributed to a network-wide repository of pictures linked to a specific individual, which included data related to gender, zip code and relative age.

B. Unauthorized Data Practices Exposed- "Thampi Study"

21. On February 8, 2012, independent researcher Arun Thampi discovered that an application they had installed on their mobile device was uploading their entire contact address book to its servers. A contact address book is a database within computing devices for storing entries called "contacts." Each contact consists of a few standard fields of data, including but not

limited to, contact names, e-mail, instant message, phone, job employer, addresses, country, state or province, postal code, website, birthday, and notes. The discovery was made by using a software tool called "mitmproxy," which relies on a common methodology referred to as the "man-in-the-middle," which analyzed data sent to and from an application in real time. The findings were reported as follows:

> "I noticed that my entire address book (including full names, emails and phone numbers) was being sent as a plist to Hipster. Now I don't remember having given permission to Hipster to access my address book and send its contents to its servers, so I created a completely new "Hipster" and repeated the experiment and I got the same result – my address book was in Hipster's hands.
> The Trail of Events
> 1. https://api.path.com/1/users.plist
> As soon as you create a new account to Hipster, a call is made to https://api.Hipster.com/1/users.plist with your first name, last name, gender and password. An plist is returned which contains the user's ID as well as other information such as the date of creation.
> 2. https://api.path.com/3/moment/feed/home?all_friends=1
> This API call uses basic HTTP authentication (with a certain key) to obtain some metadata about myself – from the binary plist file it looks like it contains my first name, last name, cover photo, profile picture, etc.
> 3. https://api.path.com/3/contacts/add
> This is the actual offending call which uploads my entire address book to Hipster.
> This is followed by normal API calls which among others, updates my location, fetches my activity stream and tracks events within the app using Mixpanel."
> Arun Thampi, "Path uploads your entire iPhone address book to its servers" February 8, 2012 (last accessed February 13, 2012), online: http://mclov.in/2012/02/08/Path-uploads-your-entire-address-book-to-their-servers.html.

22. Shortly after news related to the Thampi study was revealed, additional applications, including Defendant Hipster's App, were analyzed to determine whether the apps were also obtaining user's contact address book data without authorization.

> "**Hipster uploads part of your iPhone address book to its servers [Update Feb 9 midnight]**
> Hipster CEO, Doug Ludlow, apologies and promises updates to opt-in to email harvesting.
> (http://techcrunch.com/2012/02/08/hipster-ceo-also-apologizes-for-address-book-gate-calls-for-application-privacy-summit-guest-post/)
> **[Original post]**
> Inspired by this post (which you should all read), I looked at the apps on my own iPhone for information leakage by other apps. I figured this would be common practice, and lo and behold, when booting up Hipster, it seems like parts of my iPhone address book were being uploaded to

Hipster. Here's the breakdown, done in the style of Arun Thampi (the author of the first post).

Creating an Account

Hipster starts with a POST to **api.hipster.com/v1/people**

Worth noting, this is not over HTTPS, and it sends your info, including password and iPhone UID in plaintext. Ugh.

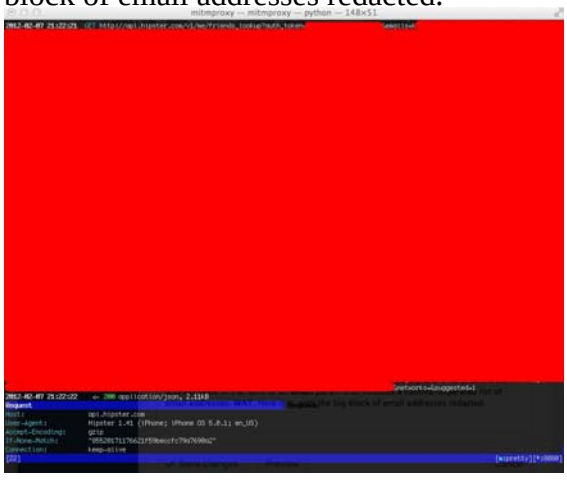
Okay, not terrible.

Several other transactions happen here, giving us acknowledgment of your login and creation of an account and user ID, and the public **"Popular"** feed is returned.

Sadly, the badness happens when you go to add your friends from the **More > Find Friends** menu option.

Badness

The Hipster app, in an unsecured HTTP GET request, sends a big chunk of your iPhone address book in the form of an **email** param that includes a comma-separated list of email addresses. **WAT**. Here it is, with the big block of email addresses redacted.



Okay, that's enormous. Let's just get the important bits. The HTTP GET goes to:

api.hipster.com/v1/me/friends_lookup?auth_token=[redacted]&emails=[…]

Boy. Thanks, Hipster.

The Issue

As was addressed in the other post, this is offensive for a few reasons:

1. Hipster never asked me for permission to send my address book emails to them.
2. Hipster does not say anything (AFAIK) about if they are storing those emails or what.
3. The Hipster app allows you to deselect the "Contacts" button when looking for new friends, but it is **enabled by default**. Therefore, there is no way to avoid sending address book emails to Hipster, as far as I can tell.

Thanks to the original article on Path. While it is up for debate how much of a negative impact this has on an individual's privacy, I feel these two examples (which were easy to come by) point toward a state of lax privacy attitudes among some of the leading edge of socially-minded consumer applications.

Time to clean up a bit, right?

Comments below, or hit me up on Twitter, @mchang"

Mark Chang Blog: more of the same, "Hipster uploads part of your iPhone address book to its servers," (Feb. 9), Last accessed December 28, 2012, online: http://blog.markchang.net/post/17244167951/hipster-uploads-part-of-your-iphone-address-book-to-its.

C. Harm to Plaintiffs and the Class

23. Plaintiffs' and Class Members' contact address data was obtained and aggregated with data, for purposes unrelated to any use of Defendant Hipster's App, and was obtained for purposes including, but not limited to, collecting and aggregating such to the uploaded digital content, and digital content created by use of Defendant Hipster's App, which included the Plaintiffs' and Class Members' "fine" geo-location coordinates, a location indicator that reveals the exact latitude and longitude of the location where the digital content was accessed or photo taken, as opposed to "coarse" location which reveals the location identifier as a city, a practice used by most applications. Defendant failed to adequately disclose, or obtain permission for such activities, within its Terms of Service or Privacy Policy. Defendant's request for the use of location coordinates failed to provide notice that such would be fine coordinates, and be affixed to uploaded pictures, and/or pictures created while using Defendant Hipster's App, nor that Defendant would code the digital content uploaded by Plaintiffs and Class Members to correlate such with geo-location libraries which revealed the exact location of Plaintiffs and Class Members to within a few feet of the location where the digital content was taken, then aggregating such with the user's contact address data in order to conduct tracking of the Plaintiffs and Class Members surreptitiously.

24. Plaintiffs and Class Members have suffered an injury in fact by the invasion of a

legally protected interest which is concrete and particularized, actual or imminent, and not conjectural or hypothetical by their use of Defendant Hipster's App.

25. The Hipster App allowed Hipster to gain unauthorized access, collection, aggregation, dissemination, use, and retention of Plaintiffs' and Class Members' contemporaneous electronic communications.

26. The Hipster App further allowed Hipster to access stored communications within Electronic Communication Service ("ECS") and Remote Computing Services ("RCS"). This was accomplished through Hipster's access to the mobile device user's contact address data, the electronic communications of the metadata within photos while being uploaded, through accessing electronic communications stored temporarily within the Plaintiffs' and Class Members' mobile devices, and through access to electronic communications stored in remote computing services when Defendant accessed Plaintiffs' and Class Members' photo metadata stored at the Amazon facility, a third party server.

27. The injury and conduct complained of is causally connected and likely to be redressed by a favorable resolution.

28. Plaintiffs and Class Members have incurred actual economic loss, a loss that is actual, non-speculative, out of pocket, sum certain; and can be scientifically documented.

29. When Defendant used Plaintiffs' and Class Members' mobile devices without notice or authorization to conduct its unauthorized collection and tracking activities for its own financial benefits, it caused actual harm that is not hypothetical, and includes, but is not limited to: (1) diminished mobile devices resources, such as storage, battery life, and bandwidth; (2) increased, unexpected, and unreasonable risk to the security of sensitive personal information; (3) "out of pocket" costs to remove embedded code from digital contact uploaded; and (4) "out of pocket" costs to re-install Exchangeable Image File Format ("EXIF"), International Press Telecommunications Council ("IPTC"), and Extensible Metadata Platform ("XMP") altered and/or deleted by Defendant.

30. Defendant's unauthorized collection of Plaintiffs and Class Members contact address data revealed contacts that includes, but is not limited to:

1) Personal contacts of highly sensitive personal information, revealing contact address data for professional treatment involving sexuality, mental illness, alcoholism, incest, rape and domestic violence;

2) Personal contacts, revealing contact address data for family, relatives, and friends, most which are not in privity with Defendant, and minor children below the age of thirteen, the collection of personal identifying information being legally forbidden;

3) Personal association contacts, revealing personal, professional and political associations, hindering, due to fear of disclosure, an individual's ability to associate for the advancement of their beliefs and ideas, the inseparable aspect assured by the due process guarantee of the Fourteenth Amendment;

4) Commercial contacts, revealing business contacts, the creation of such involves extended periods of time, labor, costs, and expertise to create; however the use of such has detrimental financial effects on the Plaintiffs' and Class Members' business, such data has an independent economic value, neither "abstract or hypothetical," and a corporate asset having inherent economic value and the mere collection and use of such data constitutes a loss of money or property.

5) Such professional contacts, revealing individuals associated with licensed professionals as doctors or lawyers that are legally obligated to keep any and all professional associations confidential, exposing them to liability and license forfeiture if such information was released in any manner.

31. Such contact address data was created by Plaintiffs and Class Members, contained within their mobile devices remote computing stored facility, and not created by Defendant or their web analytics vendor. Defendant's acquisition of this Personal Identifying Information ("PII") from Plaintiffs and Class Members through its use of the Hipster App took place as a continuous and repeated operation, as it occurred and reoccurred upon each visit to the Hipster site. Defendant's "free" app business model was a consumer deceptive practice wherein the Hipster App Freemium's "currency" was Plaintiffs' and Class Members' contact address data, fine GPS coordinates, EXIF, IPTC, and XMP data. All such information was acquired by

Hipster without notice or consent.

32. By way of further violation, the Hipster App, utilizing Metadata in photographs taken by users, created a digital dataset, linked to the user's exact location, and posted to a publicly accessible forum that revealed the user's exact fine GPS settings. This action not only violated the privacy rights of the user, but also posed a security risk. When Defendant aggregated Plaintiffs' and Class Members' contact address data for commercial purposes without notice or consent, swept up within Hipster's business model were minor children, whose photos were published without any protections whatsoever, and which publications included the exact location where the picture was taken, such as pictures of home, along with a detailed map of the home's exact location – all derivable from the photo's metadata.

D. Hipster's Mea Culpa and Subsequent Conduct

33. Defendant Hipster's CEO, Doug Ludlow, attempted to diminish the impact of its public relations nightmare by providing an immediate "Mea Culpa" of sorts, informing all users of its intent to continue to retain and store the unauthorized data in bulk, ignoring calls to delete its unlawfully obtained data, but noting how sorry it was:

> "We blew it, we're sorry, and we're going to make it right.
> It's Hipster's goal to provide a fun and beautiful service for our community to share where they are, and what they are doing – creating a safe environment for our users is of the utmost importance to us. However, when we built our "Find Friends" feature for iOS, we clearly dropped the ball when it comes to protecting our users' privacy.
> Yesterday, one of our Hipster users, Mark Chang (http://markchang.tumblr.com/) wrote a blog post detailing a few ways in which our "Find Friends" feature handles user privacy issues. You can read their post here .
> Mark's criticisms were spot on, and needless to say we're pretty embarrassed by the situation. Embarrassed not because we had malicious goals in mind (we don't store the contact data we pull – we just match it to existing users), but embarrassed by the fact that we pushed a feature that doesn't meet our standards for the protection of our user's data.
> How are we working to remedy the situation? In an update that will be available through iTunes this week, we've changed the way our "Find Friends" feature works on iOS. Rather than automatically pull in a user's contacts to help them find people already on Hipster, we're making this feature opt-in, and users will have to confirm that they want to grant access to their address book. In addition, this data will now be transferred through a SSL connection.
> But where do go from here?"
>
> "Hipster CEO Also Apologizes For Address Book-Gate, Calls For Application Privacy Summit" (last accessed April 5, 2012) online at:

http://www.ceo.com/flink/?lnk=http%3A%2F%2Ftechcrunch.com%2F2012%2F02%2F08%2Fhipster-ceo-also-apologizes-for-address-book-gate-calls-for-application-privacy-summit-guest-post%2F

34. Defendant's mea culpa failed to inform all users of its intent to continue to retain and store the previously data obtained in bulk, in lieu of deleting the data obtained to date.

35. Defendant's response that its activities were a common acceptable practice within the industry was without merit upon review of the app store guidelines since Defendant is an "Apple Developer" that agreed to the iOS Developer Agreement ("IDA"), and the Program License Agreement ("PLA"), which included the following restrictions:

> "17.1: Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used
> 17.2: Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected"
> Letter from Tim Cook of Apple Inc., to Congressmen Waxman and Butterfield, (last accessed March 12, 2012), online: http://democrats.energycommerce.house.gov/sites/default/files/documents/Letter_CookResponse_03.02.12.pdf.

36. Defendant's slogan that obtaining and retaining the contact information was necessary in order to "provide a fun and beautiful service for our community" was a false and misleading statement. In fact, it was actually not necessary to keep user data after the user has found their friends on their app, since a hashing-enabled app could delete all the uploaded hashed data, and still allow the whole "friend-finding" process to work.

37. Defendant quietly added a new pop-up requesting user authority to obtain contact address data:

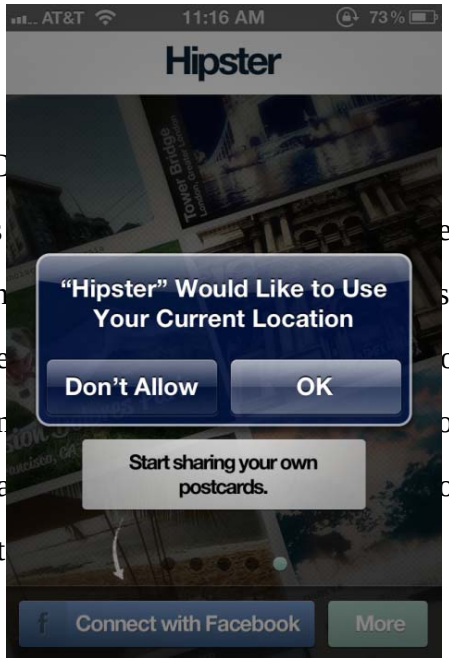
38. Defendant's claim that it even could suggest "friends" from a user's contact address book merely by those individuals being within the Plaintiffs and Class Member's contact address book was also without merit because it ignores the fact that all contacts are not all "friends."

39. Defendant's business plan concentrated on exponential growth, relying not exclusively from user only data, but on the data derived from the interactions between the user and their contacts. By calculating and pruning its users' interactions with their contacts on multiple platforms, it allowed Defendant to preserve its own platforms and servers.

40. The Hipster App was marketed to promote the app for close connections, but in actuality it allowed Defendant to ride the coattails of existing platforms, such as Facebook, which had almost a billion users. Following principles similar to those known as the "Metcalfe's Law," a principle related to the fact that a network was proportional to the square of the number of connected users of the system, Defendant's intent was exponential growth using its user's contacts.

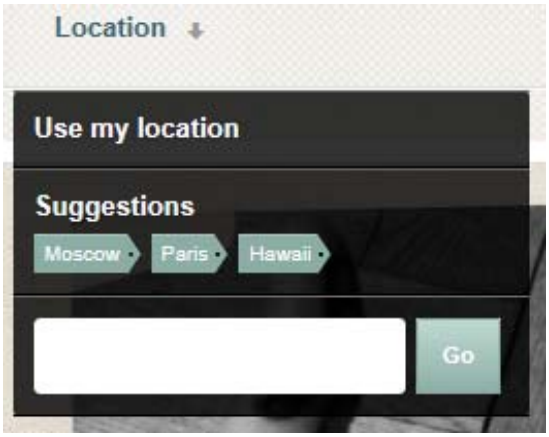
41. Defendant sought a more definitive geo-metric coordination of its members location than that which was provided by Apple and Android by means of intrusive and undisclosed geo-location techniques by using hidden data in user's photos. Such actions were

not disclosed to the Plaintiffs and C



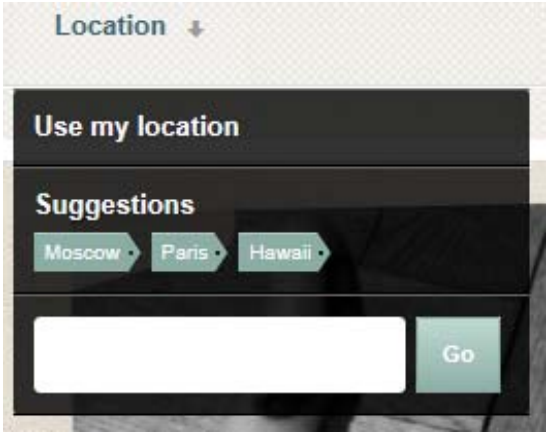
42. Defendant Hipster's e Plaintiffs and Class Members that locations used within s, not coarse locations. As such, users were given a false sense ought authorization to use the "current" location. Plaintiffs' an ow such posting of their digital content in a public forum wa o's would merely reveal "nearby" locations, since it was not

43. Defendant Hipster's App provided a pop-up entitled: "use my location," to further confuse Plaintiffs and Class Members noting a few suggestions: Moscow, Paris, Hawaii. Such provided notice to the Plaintiffs and Class Members that locations used within the Hipster App would reference coarse locations, not fine locations, since cities are noted, thus providing a false sense of security for the user when the Defendant sought authorization to use the "current" location of the user, and definitely not reference their home address with accompanying photo:



44. Defendant Hipster's App also uses the user's location at all times, drawing excessive bandwidth, a service paid for by the Plaintiffs and Class Members, without notice or consent. Hipster use of the user's fine GPS location made such data accessible by Hipster for any purpose, at anytime. Defendant thus gave itself 24/7 access to Plaintiffs' and Class Members' fine GPS location, even when the user was not uploading pictures, or not viewing

pictures, nor even visiting Defendants Hipster App.



45. The underlying purpose for Defendant Hipster's App was the data mining of computing devices to obtain Personal Identifying Information ("PII). Defendant's obtaining PII provided Hipster the ability to eliminate substantial server costs, allow access to user content created and uploaded by users, which provided an immediate established platform was further compounded by sending all of Plaintiffs and Class Members contact address data to its servers unencrypted, all without any disclosure in its privacy policy.

46. Defendant Hipster's App design architecture turns its users into unwitting data loggers, creating a commodity for sale, and providing the mechanisms required for substantial user data collection. The extent of this exploitative activity was not disclosed by Hipster, and such activities were certainly not within the contemplation of its users when Hipster stated:

> "Hipster may post on my behalf, including status updates, photos and more. Access my data any time. Hipster may access my data when I'm not using the application."

47. A certain design point of Defendant Hipster's App architecture reveals functions that involve digital content, user content, and fine GPS. The design to obtain the data is simple but quite effective to provide a mechanism for substantial user data collection and the precise tracking of users. Using photos, the most prevalent type of "digital media," Defendant's collection of user's mobile device contact address data associated with media's GPS fine location and media metatags provided abundant PII for Defendants to entice venture capital funding to continue its business model, deceptively referred to as a "Freemium" model, but in

actuality the model is based upon the exchange of property, and is better referenced as a "property-exchange" model.

48. Plaintiffs and Class Members' photos and its metadata have many of the same characteristics of property. It is property created by the user, fixed when transmitted to storage, sold and traded on a regular basis, and used as consideration in exchange for goods and services, as opposed to that is derivative user data, or data not created by the user such as data created by the user's interaction with websites, mobile apps, metric companies, and ad networks. The location-based mobile data within photo metadata has additional market exchange value between a mobile device user and third parties, including but not limited to, mobile service providers, websites, apps, and ad networks. The monetary value is created because mobile apps encourage the exchange of such to obtain discounts, rewards, and use of an app. User created data therefore exists as a property interest, and should only be exchanged at the user's discretion. Plaintiffs and Class Members "paid" for the products and services they "bought" from Defendant by providing their PII contained within their photos and its metadata, a valuable property that was exchanged not only for Defendant's products and services, but also in exchange for Defendant's promise to employ commercially reasonable methods to safeguard the PII that was exchanged. Defendant failed to employ commercially reasonable methods to safeguard the PII of its users.

49. While Defendant's practices included the unauthorized interception, use, and storage of contact address data, a review of Defendant's business activities also revealed a level of tracking unsurpassed by most apps. Defendant's "uncommon practices" included correlating the user's contact address data with digital media content containing EXIF, IPTC, and XMP data, exact GPS latitude and longitude coordinates, and user's metatags affixed to digital content, creating a new version of data tracking and "Device Fingerprinting."

50. The underlying purpose for Defendant Hipster's App was the data mining of computing devices to obtain PII, as opposed to standard platforms which limit themselves to exploitation of content aggregation. The data mining of PII provided Defendant Hipster with the ability to eliminate substantial server costs, allow access to user content created and uploaded by users, and provided an immediate established platform.

51. By bypassing any authorization or consent by the user, Defendant obtained immediate growth through the acquisition of the user's contact address data. A user's contact data contained, on average, one hundred (100) to a thousand (1,000) individuals per user. This immediate access to massive amounts of intimate data provided Hipster a "virtual asset" for marketing purposes, and Hipster used this virtual asset to solicit funding by venture capitalists.

52. Defendant utilized the services of Amazon Web Services ("AWS"). AWS is a suite of cloud-based, pay-as-you-go, on-demand services that facilitate building web applications by providing the primary infrastructure components. With AWS, developers can rapidly provision, and scale as needed, computing resources, storage, and even messaging. AWS supports the development and consequent deployment of entire web architectures — ranging from the actual hardware infrastructure for entire web applications to reside to content delivery networks.

53. Defendant reportedly sent all Plaintiffs' and Class Members' data to AWS, including but not limited to, Plaintiffs' and Class Members' contact address data, and on a continuous basis, re-accessed the contact address data that it had no authority to initially obtain. Like a thief that steals property, only to use the pawn slip to re-acquire the stolen property, Defendant had no authority to initially acquire Plaintiffs' and Class Members' contact address data, nor authority to re-acquire such data from the Amazon remote computing services.

E. <u>Defendant's Unauthorized Use of Metadata</u>

54. Prior to the emergence of mobile devices apps, online tracking on computers involved using HTTP cookies implanted within the digital content on websites. An HTTP cookie is data stored on a computer that assists in automated access to websites and may also be used for user tracking, browser history, and storage of PII, for market research of behavioral targeting in advertising. Once an individual viewed website content, their computer became a "host" to carry the tracking mechanism. The use of cookies for tracking within mobile devices though presented a multitude of functional problems, thus Advertising Networks and Web Analytic Vendors sought a mechanism to allow user tracking, preferably a mechanism that would require a method to identify mobile devices. Unique Device Identifiers ("UDIDs"), an actual number printed

within the mobile device, provided such an identifier because it was a device-specific identifier that could be unified across apps and servers, thereby uniquely identifying a mobile device, and eventually a user. With the emergence of mobile device applications in 2008 there existed an ability to substantially track users on mobile devices using UDIDs; however a public outrage erupted when it was reported UDIDs were also being linked to the user's GPS settings. The result was the deprecation of UDIDs, so a new "work-around" to allow tracking users was required by advertising companies and their software providers. The use of metadata within photos permitted this new tracking mechanism.

55. Metadata is a term that describes information embedded within an image or other type of file, and is basically data about data. It is used as a method to store information that can transfer with the file. One type of metadata is information that is added to digital photos on image files at the instant of exposure. This metadata includes, but is not limited to, characteristics of the photo, copyright information, caption, credits, keywords, creation date and location, source information, and exposure time.

56. While transferring photos from one format to another may require transcoding, a direct digital-to-digital data conversion of one encoding to another, i.e. reformatting file size, Defendant's advertised "filter service" was more about obtaining a function that obtained the user's fine geo-location coordinates while the user waited unknowingly to see their pictures "filtered." The embedded metadata contained the precise longitude and latitude of the mobile device when the photo was taken. Called "geo-tagging," this relatively recent phenomenon uses GPS technology in certain computing devices with cameras to add hidden map coordinates to digital photographs, and other digital media.

57. Defendant's actions involved obtaining Plaintiffs' and Class Members' contact address data and GPS coordinates. This data was aggregated into the digital content (photo) metatags. Additional aggregated metadata included, but was not limited to; a user's full name, exact GPS location within a few feet, user's unique identifier, and an etag header. All of this information was cached.

58. Defendant was granted a Limited License to publicize the Plaintiffs' and Class

Members' photos, including permission to access designated photos within their mobile device's photo library, and/or photos taken while accessing Defendant Hipster's App. However, such Limited License did not permit Hipster access to, deletion, modification, use, dissemination, and storage, of all metadata in all photos. Defendant Hipster's access to, deletion, modification, and use of Plaintiffs' and Class Members' metadata within their photos, was all undertaken without notice or consent.

F. Photo Metadata requires Removal, Repair, and Replacement

59. To remove, repair, or replace the photos altered by Defendant's App constitutes an economic harm that is actual, non-speculative, out of pocket, sum certain, and it can be scientifically documented.

60. Defendant has altered, deleted or added metadata within the Plaintiffs and Class Members digital content, These alterations, deletions, and additions now requires removal, repair, and replacement. Like a toxic oil spill in the Gulf of Mexico causing loss and/or damage to the area residents, embedded "toxic filter cookies" now require a "toxic filter cookie cleanup."

61. Plaintiffs' and Class Members' photos are personal property that cannot be replicated. Plaintiffs and Class Members cannot delete the metadata now contained within their photos, and correlated to their contact address data, merely by selecting a browser cleaner used to clean cookies. Complicating the cleaning process is the fact that all Plaintiffs' and Class Members' photos stored within their computer device's memory include photos not uploaded within Defendant Hipster's App, thus each photo shall need to be examined. Plaintiffs and Class Members demand that Defendant return the digital content within their computing devices to the state that existed prior to any and all activity implemented by Defendant including, but not limited to, removal of all fine GPS coordinates attached to their digital content. Such a demand is premised on the fact that it creates a tracking mechanism that shall exist on Plaintiffs' and Class Members' devices until it is removed.

62. Defendant's actions have caused harm to the Plaintiffs and Class Members including, but not limited to, loss due to costs associated for the requirement of computing device forensics to investigate, locate, and delete any and all tracking mechanisms located within

Plaintiffs' and Class Members' mobile devices.

63. Plaintiffs and Class Members use their mobile devices' memory to store and use digital content. Plaintiffs and Class Members do not want to use the mobile devices' software to delete their entire memory but only delete that data within their hardware associated with Defendant and its Affiliates. To do so, however, requires accessing the Plaintiffs' and Class Members' mobile device's memory to examine each and every data file pertaining to digital content.

64. Plaintiffs and Class Members have suffered loss and/or damages in order to mitigate Defendant's invasive actions by expending time, money, and resources, to investigate and repair their computing devices, a process requiring the examination of all digital content uploaded to Defendant Hipster's App.

65. Plaintiffs' and Class Members' economic loss now requires that they incur costs to obtain a complete forensic examination of their mobile devices similar to the costs incurred to conduct such analysis for a personal computer:

66. The average mobile device includes 16 GBs of memory (an 80 GB hard drive is generally included in personal computers). Taking into consideration the GB hard drive reduction, estimates for such services for Plaintiffs and Class Members shall exceed seven hours at a cost of three hundred and fifty dollars ($350.00) per hour, or exceeding a total cost of two thousand four hundred and fifty dollars ($2,450.00) per device.

67. Plaintiffs' and Class Members' most substantial economic loss involves the costs that will be incurred to hire an expert to review each photo accessed by Defendant, uploaded to Defendant's app, and transmitted to the cloud computing facility, to extract and delete any and all Defendant tracking data added to Plaintiffs' and Class Members' digital media content (photos). Additional costs must be incurred to manually reinstall the EXIF, IPTC, and XMP data which existed prior to the unauthorized access by Defendant and which was deleted by the Hipster App.

68. The average costs of mobile devices range from one hundred and fifty dollars ($150.00) to five hundred dollars ($500.00). Any interference of any kind to such devices would

interfere with their personal enjoyment and use. Plaintiffs and Class Members were harmed due to any delay in use once the Defendant's actions became known, delay in time to investigate and repair any loss and/or damage.

69. Plaintiffs and Class Members purchased computing devices with consideration about costs, speed and security features. The cost of the hardware and software necessary for the security features were factored into the total price of the computing devices, thus a specific sum was allocated to the cost of including the security features. As such, Defendant's circumvention of their computing devices rendered such hardware and software protections purchased within the computing device worthless.

70. Native Security Software was provided to Plaintiffs and Class Members within their computing devices when purchased for use on a trial basis, generally an average sixty (60) day trial period. Common Native Security Software is a Norton or McAfee product. Once the trial period expired, the Plaintiffs and Class Members download software or purchased such at an electronic store. Security Software costs averages approximately seventy five dollars ($75.00) to one hundred and fifty dollars ($150.00) per device to provide continued security protection. Such security software purchased was rendered worthless, or substantially reduced in value, due to the Defendant's activities described herein that form the basis of this action.

71. As a result of Defendant's conduct, Plaintiffs and Class Members will be required to purchase a hard drive to enable the transfer of files and re-installation of the operating system on their mobile devices. A retail price for this would average one hundred dollars ($100.00) for the hard drive and approximately one hundred forty nine dollars ($149.00) to two hundred forty nine dollars ($249.00) for the operation of transferring the files, installing Windows, etc. or about three hundred dollars ($300.00) to three hundred fifty dollars ($350.00) in total.

72. As a result of Defendant's conduct, Plaintiffs and Class Members will be required to hire a computer technician to spend many hours reviewing every single digital photo file to identify and delete Defendant's tracking mechanisms. Although such a procedure may appear inefficient, the value to Plaintiffs and Class Members of their original, unmodified photos are of inestimable value, and are irreplaceable.

73. As a result of Defendant's conduct, Plaintiffs and Class Members who still wish to use the infected hard drive must extract all the authorized data and transfer it to another hard drive, while the original infected drive is sanitized. Data transfer costs as much as about two hundred fifty dollars ($250.00). Plaintiffs' and Class Members' loss includes a cost of up to three hundred fifty dollars ($350.00) for the hard drive and this service. Most mobile device technicians will not re-install all of the programs for the user. Re-installing an average user's applications is estimated to take another three (3) to four (4) hours at a potential cost of four hundred dollars ($400.00). Market cost to buy a new hard drive and have all of a user's programs and files transferred to it, so that they were made whole and in the same shape that they were before the unauthorized modifications imposed by the Hipster APP would cost an estimated seven hundred fifty dollars ($750.00).

74. The economic harm to Plaintiffs and potentially millions of Class Members includes loss of their data. This data has economic value; Facebook recently set a baseline for the value of class data at ten dollars ($10.00) per user.

> Michele Bowman, "Facebook Users' Privacy Is Worth $10 Each," December 7, 2012, (last accessed December 8, 2012), online: http://blogs.lawyers.com/2012/12/facebook-privacy-worth-10/.

75. Plaintiffs will need discovery before being able to provide additional details about the total extent of the economic harm to Plaintiffs and Class Members, including but not limited to, harm to their photos, its metadata, and any additional costs to remove, repair, and replace such property. Defendant Hipster's App utilizes highly advanced technology. It would be unrealistic, and unjust, for a court to require the Plaintiffs to provide precise, technical details concerning all activities of Defendant by identifying each type of personal data the Defendant obtained, collected, generated, derived, disseminated, stored, or caused to be stored; and aggregated with Plaintiffs' and Class Members' contact address data that created economic harm to Plaintiffs and Class Members since Defendant's company operated without public disclosure of its activities. Nevertheless, the Complaint provides sufficient facts to draw a reasonable inference that the Defendant caused property damage to Plaintiffs' and Class Members' property.

G. Defendant's Tracking of Users

76. Defendant's tracking of users constitutes economic harm that is actual, non-speculative, out of pocket, sum certain, and can be scientifically documented.

77. Defendant failed to disclose to its user's that their contacts would be monitored and used to track and store information regarding consumers' mobile activity. The installation of such tracking capabilities would be material to consumers in their decision whether to install the software offered by Defendant.

78. Without remedy, Plaintiffs and Class Members will continue to be tracked by Defendant and possibly dozens of companies — companies they've never heard of, companies they have no relationship with, companies they would never choose to trust.

79. The tracking and monitoring of mobile device users' contacts will have a negative effect on individuals' access to information. The anonymity that the Internet affords individuals has rendered it an invaluable resource for those seeking out information. Particularly where the contact address book data relates to contacts associated with Plaintiffs and Class Members including controversial topics such as sex, sexuality, or health issues such as HIV, depression, abortion, political association – the ability to access information without risking identification has been an essential aspect of internet access. The pressures placed upon anonymity by artifacts such as Defendant has designed will result in increased pressure on individuals to permit the collection of contact associations and other information that can be tied to them, as a quid pro quo of engaging in transactions and interactions online, thereby placing a burden on individuals who choose to protect their privacy.

H. Transmission "In the Clear"

80. Not only was Plaintiffs' personal information transmitted to the Defendant, but all of Plaintiffs' contact address data was transmitted "in the clear" (sometimes referred to as "plain text"): that is, without encryption. Defendant could have generated a "hash" of the e-mail addresses to provide a unique identifier. This would have allowed the matches necessary for friend finding, while being incapable of being converted back into the original address. According to the National Institute for Standards and Technology (NIST), "Mobile devices have a broad attack surface including Bluetooth, Wi-Fi, and cellular communications interfaces as

well as protocols for Web transactions," and "[s]ensitive data should be encrypted during data transmission and when stored on the device or in external memory cards." Wayne Jansen, Karen Scarfone, Recommendations of the National Institute of Standards and Technology: Guidelines on Cell Phone and PDA Security, U.S. Dept. of Commerce, NIST, SP 800-124 at 3-2 (Oct. 2008).

81. Defendant's transmission of user data "in the clear," was substandard in light of reasonably accepted security measures, exposing Plaintiffs' and Class Member's personal information to unreasonable risks of interception that are well understood to be associated with such poorly secured transmission. Such unsecured transmissions were particularly inappropriate given the nature of mobile devices and Apps through which such information was transmitted.

I. Collection of Private and Personal Data That Did Not Belong To Hipster

82. The personal and private contact address book data is of extreme interest to many advertising networks and web analytics companies, including the Defendant.

83. When users download and install Defendant's App on their mobile devices, the Defendant's software accesses personal information on those devices without users' awareness or permission and transmits the information including, but not limited to, cell phone numbers, address books, UDIDs, and geo-location histories— highly personal details about who the consumers are, who they know, what they do, and where they are.

84. With the contact address book data acquired, the Defendant could use the information to compile personal, private, and sensitive information that included their personal characteristics such as gender, age, race, family status, education level, geographic location, and household income, and other highly sensitive, non-pubic information even though the Defendant requires none of this information to provide the user services for which the Apps were marketed.

85. The Defendant acquired contact address book data and compiled profiles that were unnecessary to the Apps' stated functions but were useful to the Defendant in their commercial compilation, use, and sale of consumers' personal information.

86. Plaintiffs did not consent to being personally identified to the Defendant or for their personally identifiable information to be shared with and used on behalf of the Defendant.

87. The Defendant's actions were surreptitious and deliberately hidden, and were conducted without authorization and/or exceeding any authorization that may have been given.

J. Allegations Supporting Violations of Consumer Statutes and Fraud Claims

88. Plaintiffs and Class Members are "consumers" because they acquired Defendant's App for personal purposes, and the Defendant Hipster App they downloaded qualifies as tangible "goods." Plaintiffs' and Class Members' claims are premised on the fact that Defendant misrepresented that it designed Defendant Hipster's App exercising tight control over the development and marketing for Apps to be used on such devices, with adequate safeguards to ensure the privacy and security of Plaintiffs' and Class Members' personal information residing on their mobile devices.

89. Defendant provides a "service" to Plaintiffs and Class Members permitting use of its platform, acting as "hosting" service for digital content, unlike "free" mobile applications that provide content to users in order to obtain user's PII. Defendant does not provide content, such is provided by the Plaintiffs and Class Members. Plaintiffs and Class Members and Defendant are mutually bound by contract, permitting the Plaintiffs and Class Members to upload copyrightable content to the Defendant's platform.

90. Defendant engaged in unfair and deceptive acts and practices in connection with the marketing of Defendant Hipster's App to Plaintiff. Defendant's past and ongoing acts and practices include, but are not limited to, the following material misrepresentations and omissions with respect to the quality of Defendant Hipster's App and the Defendant ecosystem:

- Defendant Hipster's App claimed to be a "free app" when in fact, Defendant Hipster's App was not truly free because Defendant obtain Plaintiffs' valuable information assets, and consumed their bandwidth and resources, such as memory storage and battery life, without consent or notice.
- Plaintiffs could not prevent Defendant from collecting Plaintiffs' data about them by switching the privacy settings on their computing mobile devices to "Off," when, in fact, Defendant continued to obtain

contact address book data about users even when privacy setup was set to restrict access.

91. Plaintiffs relied upon and were deceived by these material misrepresentations and omissions. Plaintiffs and the Class would not have downloaded Defendant Hipster's App if Defendant had disclosed the true facts that it would surreptitiously obtain from their mobile device using Defendant Hipster's App as a conduit to obtain such contact address data and consume portions of the "cache" and/or gigabytes of memory on their devices—memory that Plaintiffs paid for the exclusive use of when they purchased their mobile device and their mobile plan. Plaintiffs were misled into downloading Defendant's product that did not meet their reasonable expectations. Given the undisclosed costs imposed by the bandwidth used by Defendant Hipster's App, for purposes unrelated to the use of the Defendant's app, it was not as useful to Plaintiffs and was not as valuable to them for the bandwidth use for which they paid. As a proximate and direct result of Defendant's misrepresentations, Plaintiffs and Members of the Class have been injured and suffered damages in that they have downloaded a product that invaded their privacy, rendered their personal information insecure, and consumed their valuable device storage and powered resources as well as their Internet bandwidth.

92. Plaintiffs and Class Members were deceived into downloading a product that did not operate as represented by Defendant. Plaintiffs and Class Members purchased computing mobile devices costing in excess over $150. Included in this purchase price was access to thousands of third-party software applications available in App Stores and markets. Defendant specifically and intentionally induced the downloading of its Hipster App by Plaintiffs and Class Members by offering an ostensibly "free" App. Defendant, however, failed to disclose that its Hipster App included spyware that utilized Defendant-provided tools to collect Plaintiffs' and Class Members' personal information. Had Plaintiffs and the Class known of Defendant's practices, they would not have downloaded the Hipster App which now has substantially devalued Plaintiffs' and Class Members' mobile device by such undesirable practices. Additionally, Defendant's competitors manufacture, market, and distribute comparable mobile apps that do not collect contact address data without permission and without adequate disclosure

of those material facts. Plaintiffs and Class Members suffered actual damages as a result of Defendant acts and omissions.

93. Defendant failed to disclose the material privacy and security characteristics of Defendant Hipster's App and its operation within the Defendant-controlled ecosystem because it: (i) knew or should have known about such characteristics at the time that Plaintiffs and members of the Class downloaded the product, inasmuch as Defendant created the Defendant's app; (ii) had exclusive knowledge of these material facts, which information was not known to Plaintiff; and (iii) made a partial representation as to Defendant Hipster's App integrity in promoting Plaintiffs' privacy and security interests and interests in the reasonably expected utility of their Defendant Hipster's App, but failed to disclose the material fact that Defendant Hipster's App, and the entire Defendant ecosystem was designed to foster the unauthorized taking of and profiting from Plaintiffs' personal information. Plaintiffs would not have downloaded Defendant Hipster's App had they known that the device would be used for such purposes.

94. Plaintiffs relied upon Defendant's representations with respect to downloading of their Defendant Hipster's App, the availability of a 'free' App, and Defendant's collection practices. Such was an important factor to Plaintiffs in making the decision to download the Hipster App, and the omission of material facts to the contrary would have resulted in the Plaintiffs making a different decision with respect to downloading the Hipster App.

95. Defendant's *modus operandi* constitutes a sharp practice in that it knew or should have known that consumers care about the status and security of personal information and privacy but are unlikely to be aware of and able to detect the means by which Defendant was conducting itself in a manner adverse to its commitments and users' interests, through the undisclosed functions of Defendant Hipster's App and the related conduct, a material misrepresentation per the FTC guidelines related to "free" products, "FTC guide concerning use of the word "free" and similar representations" http://www.ftc.gov/bcp/guides/free.htm.

K. Defendant's Unauthorized Use of Bandwidth

96. Bandwidth is the amount of data that can be transmitted across a channel in a set amount of time. Any transmission of information on the internet includes bandwidth. Similar to

utility companies, such as power or water, the "pipeline" is a substantial capital expenditure, and bandwidth usage controls the pricing model. Hosting providers charge users for bandwidth because their upstream provider charges them and so forth until it reaches the "back bone providers." Retail providers purchase it from wholesalers to sell to its consumers.

97. Bandwidth to the computer is like gasoline to a motor vehicle; without it the device is inoperable. Defendant requires bandwidth to conduct consumer tracking; however the bandwidth Defendant used belonged to the Plaintiffs and Class Members, because they were the ones who purchased it. Imagine an individual fills up their car's gas tank one day only to find it empty the next day because their neighbor drove their car out at night without their permission. Individuals pay monthly bandwidth use fees for their own use but not by third parties to conduct their tracking business. Defendant's unauthorized use of Plaintiffs' and Class Members' bandwidth relates to the use of the mobile device's functions to operate the tracking mechanism and for "calls" to "pull" contact address data and geo-location data.

98. Limiting bandwidth resources to reduce individual and corporate expenditures is sought after by all parties. Plaintiffs and Class Members average $29.99 to $79.99 per month or $479.88 to $959.88 per year for bandwidth use. Bandwidth use by the Defendant reduces the amount of bandwidth available to the user. Such use caused an economic harm to the Plaintiffs and Class Members that is actual, non-speculative, sum certain, and scientifically documentable in that:

a. Plaintiffs and Class Members purchased a monthly limited bandwidth data plan for their computer from their carrier;

b. Plaintiffs and Class Members then downloaded and accessed Defendant's App to their mobile devices, "expecting" and agreeing to limited bandwidth consumption required and necessary to interact with the Defendant Hipster App;

c. However Defendant then redirected Plaintiffs' and Class Members' mobile device to access Defendant's servers to "pull" their contact address data, and such was not "expected" by the user, *not* required to interact

with the Hipster App, *not* agreed upon by the user, and *not* necessary to operate the mobile device;

d. Defendant then made "calls" directing Plaintiffs' and Class Members' mobile devices to send contact address data on a repeated and continuous basis, thereby depleting the purchased and linked bandwidth data plan of the Plaintiffs and Class Members, and such was *not* "expected" by the user, *not* required to interact with the Hipster App, *not* agreed upon by the user, and *not* necessary to operate the mobile device.

99. "Unlimited bandwidth" plans are not actually unlimited. Major provider plans may refer to their plans as unlimited for marketing purposes, but the plans have limitations, usually noted in a footnote or link to another page discussing the limitations as to usage amounts. Providers could not possibly allow "unlimited" plans because servers do not have unlimited amounts of space. "Unlimited" data plans used to be unlimited until people started to figure out how to "tether," a method for connecting a computer to the internet via an internet-capable mobile phone. The term "unlimited" is now used to define what is considered to be more than a reasonable amount of data allotment.

100. Network providers' data plans charge consumers based upon such items as usage and "caps," i.e. $30.00 per month for an unlimited plan is standard; but limited plans have caps, such as 256 GB per month. Some national providers charge $1.00 per GB of bandwidth exceeding a certain cap. Whether the data plan is marketed as "unlimited" or "limited," the costs for the plans are allocated based upon the bandwidth usage. Thus, as the standard use of bandwidth increases, so too does the plan costs. Since plans are based upon user's average use, as consumer's usage increases collectively, costs increase for all users, while individual bandwidth overages can be costly.

101. Applications consume vast amounts of bandwidth which results in slowing a user's internet connection by using their bandwidth and diminishing the mobile devices battery life. Web Analytics devour more bandwidth than ads by accessing bandwidth to download and run ad script, thus Plaintiffs and Class Members that did not access ads on a website still had the

Defendant use their bandwidth for its tracking:

> "When you're probing, you're using a users battery and data when they don't know about it, but it's a faster way to build up data cause you're not waiting for the user to check in a few times a day. You're pinging in 100 times a day…."

Yarow, Jay "Everything You Need to Know About How Phones are Stalking You Everywhere" (last accessed June 16, 2011), online: http://www.businessinsider.com/skyhook-ceo-2011-4#ixzz1PTSNQ1pq

102. Defendant's use of the Plaintiffs' and Class Members' bandwidth for its data mining activities is similar in nature to a practice called "hot linking;" wherein one server uses another server's bandwidth to send data. While it slows down the server, it also allows bandwidth costs to be transferred to another server. While only the tech savvy individuals are aware that their mobile devices are used as a server without their knowledge or consent, fewer individuals are aware of the extent that entities make "calls" to "push" and "pull" user data to websites application services, ad networks, web analytic vendors. Defendant's data mining activities produces similar unauthorized bandwidth use.

103. Excluding the amount of bandwidth that the Plaintiffs and Class Members use, the amount necessary to operate their mobile device, interact with their apps, and the expected amount by the user's interaction with the Hipster App that was agreed upon, Defendant's unauthorized data mining activities caused substantial bandwidth use to the Plaintiffs and Class Members that resulted in actual out of pocket expenditures.

L. Unauthorized Use of Device

104. The unauthorized, surreptitious collection of Plaintiffs' and members of the Class's contact address data book injured Plaintiffs and members of the Class because the Defendant's actions consumed, and utilized power resources to which Plaintiffs and members of the Class had the right of controls and use.

105. Defendant caused injury and damage to Plaintiffs' and Class Members' mobile devices' finite resources, depleted and exhausted its memory, thus causing an actual inability to use it for its intended purposes. Defendant caused significant unwanted CPU activity, usage, and

network traffic.

106. Defendant caused injury and damage to the Plaintiffs and Class Members including, but not limited to, consumption of their device's finite resources, memory depletion, and bandwidth, which resulted in the actual inability to use those finite resources for their intended purposes. Defendant utilized Plaintiffs' and members of the Class's bandwidth resources for which Plaintiffs and members of the Class's paid charges to their carriers, and consuming storage space on his mobile device, which Plaintiffs and members of the Class had purchased without expectation of such unauthorized resource use by Defendant's App.

107. As a result, Plaintiffs and members of the Class had the resources of their mobile devices consumed and diminished without permission. Such resources were measurable and of actual value, and included mobile devices storage, battery life, and bandwidth from Plaintiffs' and members of the Class's wireless services providers. The monetary value of the resources taken from Plaintiffs and members of the Class is capable of quantification. The rate at which battery charge was diminished on the mobile devices as a result of the Defendant's actions was material to Plaintiffs and members of the Class, particularly given the power resource constraints on the mobile devices: the Defendant's repeated actions during App executions utilized approximately two to three seconds of battery capacity with each action due to the power requirements of CPU processing, file input and output actions, and Internet connectivity. Operating multiple times per day, multiplied over millions of devices, Defendant Hipster's App consumed hundreds of hours of battery life.

108. Not only did Defendant's actions cause Plaintiffs' and members of the Class's computing devices, batteries to discharge more quickly, rendering the computing devices less useful given power constraints, but Defendant's repeated actions also resulted in lasting impairment because, by repeatedly utilizing power and causing Plaintiffs to have to re-charge their computing devices batteries sooner, the Defendant shortened the actual utility and life of the mobile devices batteries, for which charging capabilities are diminished over repeated re-chargings.

109. Quantification of the effect of the Defendant's impairment of the utility of

Plaintiffs' and members of the Class's mobile device batteries and concomitant diminution in the value of the mobile devices can be discerned through discovery and expert testimony.

110. Plaintiffs will need discovery before being able to provide additional details about the total extent of economic harm to Plaintiffs and Class Members that used Defendant Hipster's App. Most of Defendant's operations were implemented without public disclosure of its activities, failing in part to reveal all procedures or means by which each type of personal data was collected, generated, or derived while using Defendant Hipster's App and aggregated with online or offline sources. It would be unrealistic, and unjust, for a court to require the Plaintiffs to provide precise, technical details concerning Defendant's complete operations without discovery. Nevertheless, the Complaint provides sufficient facts to draw a reasonable inference that Defendant caused Plaintiffs and Class Members economic harm that was actual, non-speculative, out of pocket, and ascertainable.

M. Defendant Accessed Plaintiffs' and Class Members' Electronic Communications

111. Defendant intentionally intercepted, or endeavored to intercept, Plaintiffs' and Class Members' Electronic Communications. 18 U.S.C. § 2511(1). Plaintiffs did not consent to Defendant's interception of communications within their contact address data, photo metatags, and third party cloud servers. Defendant's interception of Plaintiffs' and class member's communications was for a criminal or tortious purpose.

112. Defendant's initial interception of Plaintiffs' and Class Members' Electronic Communications occurred both external to, and internally within, Plaintiffs' and Class Members' mobile devices, including but not limited to the following:

a. Defendant's interception of Plaintiffs' and Class Members' Electronic Communications occurred internally within the Plaintiffs' mobile device when Defendant obtained Plaintiffs' contact address data, and photo library data. The Plaintiffs' contact address book is not a static file that simply sits in electronic storage, but is a file that is constantly being updated and transmitted to sync Plaintiffs' contacts with their e-mail

account, a communication that is capable of acquisition contemporaneously with transmission;

b. Defendant's interception of Plaintiffs' and Class Members' Electronic Communications occurred internally within the Plaintiffs' and Class Members' mobile device when Defendant obtained any updates of "events" to the Plaintiffs' contact address data, and photo library data;

c. Defendant's interception of Plaintiffs' and Class Members' Electronic Communications occurred internally within the Plaintiffs' and Class Members' mobile devices when Plaintiffs and Class Members' used their mobile devices photo function to take a photo when not using Defendant's app and Defendant allowed access to the fine GPS coordinates to be added to the photo's metadata, without Plaintiffs' and Class Members' notice or authorization, storing the digital content within the photo library, and such was obtained by the Defendant;

d. Defendant's interception of Plaintiffs' and Class Members' Electronic Communications occurred internally when Plaintiffs' and Class Members' used their mobile device's photo function while using the app and Defendant allowed access to the Plaintiffs' and Class Members' fine GPS coordinates that were added to the photo; without notice or authorization by the Plaintiffs' and Class Members';

e. Defendant's interception of Plaintiffs' Electronic Communications occurred internally when Defendant accessed Plaintiffs' and Class Members' contact address database, a database that is not static, without notice or authorization by the Plaintiff;

f. Defendant's interception of Plaintiffs' and Class Members' Electronic Communications occurred externally when Plaintiffs used Defendant's cloud storage for their mobile device data and Defendant accessed this remote storage server, without notice or authorization by the Plaintiffs and Class Members.

N. <u>Defendant accessed Plaintiffs' and Class Members' Stored Communications</u>

113. The Stored Communications Act covers two types of entities: (1) "remote

computing services" ("RCS"), and (2) "electronic communication services" ("ECS"). 18 U.S.C. § 2702(a)(1)-(2). The Stored Communications Act prohibits an entity "providing remote computing service to the public" from "knowingly divulge[ing] to any person or entity the contents of any communication which is carried or maintained on that service." 18 U.S.C. § 2702(a)(2).

114. Plaintiffs' and Class Members' mobile devices are a "facility," as defined within the Stored Communications Act, 18 U.S.C. § 2701, ("SCA"), referencing a facility through which an electronic communication service is provided that allows the storage of highly personal information.

115. The SCA prohibits an entity "providing remote computing service to the public" from "knowingly divulge[ing] to any person or entity the contents of any communication which is carried or maintained on that service." 18 U.S.C. § 2702(a)(2). On the other hand, under the SCA, the term "remote computing service" means "the provision to the public of computer storage or processing services by means of an electronic communications system."

116. The Stored Communications Act's provisions governing electronic communication services (ECS) is broadly defined to mean nearly any form or style of communication, including "signs, signals, writings, images, sounds, data or intelligence of any nature," obligating a service provider to hold the electronic communication in "electronic storage." The Act limits "electronic storage" to mean (1) "temporary, intermediate storage . . . incidental to the electronic transmission" of the communication and (2) copies made by the service provider for "backup protection."

117. "Information," as defined within the Act, encompasses Plaintiffs' and Class Members' contact address data stored on a user's mobile device, information held in 'electronic storage' for purposes of the SCA.

118. Defendant violated the SCA by collecting temporarily stored contact address data from the mobile devices belonging to Plaintiffs and Class members. Defendant retrieved information from their computing mobile devices revealing their contact address book data information.

119. Mobile device data is the content of a communication in 'electronic storage' as that term is used in the SCA. Defendant accessed electronic communications while in electronic storage by collecting mobile device data from Plaintiffs and Class Members without authorization. Mobile device data on mobile devices is temporarily stored, in part, pending use or delivery to an email server (who is the intended recipient, not Defendant) to access the mobile device data for its use when e-mail is sent via the mobile device, and to sync and update. Defendant violated the SCA by collecting this temporarily stored mobile device data from Plaintiffs' and Class Members' mobile device, was "in electronic storage," and therefore was accessed while in temporary "electronic storage."14 18 U.S.C. § 2510(17)(A).

120. Contact address book data on a mobile device is the content of a communication in 'electronic storage' as that term is used in the SCA. Defendant accessed electronic communications while in electronic storage by collecting contact address book data from Plaintiffs and Class Members without authorization. Contact address data on mobile devices is temporarily stored, in part, pending use or delivery to an email server (who is the intended recipient, not Defendant) to access the contact address data for its use when e-mail is sent via the mobile device, and to sync and update. Defendant violated the SCA by collecting this temporarily stored contact address data from Plaintiffs' mobile device.

121. Defendant's access to, and continuous operation to collect stored communications from the Plaintiffs' and Class Members' mobile devices was an intentional coding procedure, ignoring privacy and security settings imposed upon the mobile device by its owner, and involved an intrusion into the mobile device's memory.

122. Mobile devices were designed to maintain a database subset (cache) of the crowd-sourced Wi-Fi hotspots and cell towers around users' current location to assist in location services. Such data was collected and stored temporarily within the users' "consolidated .db" file within mobile devices. The location History Database that is accessed to embed metadata within Plaintiffs' and Class Members' digital content is derived from a process that utilizes additional databases and is created by different functions. Mobile tracking of users' by use only of data

derived from crowd-sourced Wi-Fi hotspots would be unable to precisely locate the user; however Defendant's access to, and use of, Plaintiffs' and Class Members' location history database that is derived from recorded "events," i.e. tracking of a photo, would provide the precise identification of the user to within a few meters of their location, and allow tracking.

123. The history data is stored by the history database storage. The History Database stores "events" regarding the movement of users within the geographical area, and the History Database is continually collected by the operating system in the location history database. The accuracy is an estimate of a location that is commensurate with the amount of historical information gathered and processed. The geographical information and historical data are combined to improve the accuracy of determining the location of a user.

124. The continuous update of the History Database and access to such database in "real time" provides the basis in part for Plaintiffs' and Class Members' claim that Defendant's interception was contemporaneous with the transmission of location coordinates.

125. The location history database coordinates can be derived from sources which include, but are not limited to, the mobile device's iOS, pushed to the device by a carrier or Defendant, or obtained by Plaintiffs and Class Members or an application activated by an "event," such as photo when taken or uploaded by Plaintiffs' and Class Member. Such digital content was then stored within the users' photo library on the mobile device. Defendant obtained such from storage within the mobile device.

126. Defendant tags the Plaintiffs' and Class Members digital content such as photos with the exact latitude, longitude and timestamp storing such data in the mobile device's photo library. Defendant accessed this data within the Plaintiffs' and Class Members' photo library and/or within digital content taken by the use of Defendant Hipster App without permission, and/or exceeding any permissions granted. The digital content metadata captured by Defendant includes, but is not limited to, exact latitude, longitude, and a time stamp. The interception of and access to these electronic communication occur both exterior to and within the Plaintiffs' and Class Members mobile devices. None of this access was necessary for the provisions of the ostensible purposes of the Hipster App.

127. The underlying mechanism for Defendant's unauthorized collection was the API which allowed the monitoring of Electronic Communications, between the Plaintiffs and Class Members and their databases, since the API was used to query the location history database. Defendant's API operates in the "background" without the user's knowledge. Defendant obtained Plaintiffs' and Class Members' fine GPS location under false pretenses.

O. Defendant Accessed Plaintiffs' and Class Members' Data in a Remote Computing Service ("RCS")

128. Amazon Web Services ("AWS") is a collection of remote computing services (also called web services) that together make up a cloud computing platform, offered over the Internet by Amazon.com. Heroku is a cloud platform as a service supporting several programming languages. Heroku is owned by Salesforce.com

129. Defendant used the Remote Computing Services of Amazon Web Service to reportedly store all Plaintiffs' and Class Members' data, including but not limited to, contact address data. Defendant was not authorized to obtain the Plaintiffs' and Class Members' contact address data, nor send such to the Amazon Remote Computing Service for storage; furthermore Defendant had no authority to re-access such data on a repeated and continuous basis.

130. The term "remote computing service" is defined in the ECPA as "the provision to the public of computer storage or processing services by means of an electronic communication system." 18 U.S.C. S 2711(2).

131. Defendant's servers were acting as a "remote computing service" processing or storing Plaintiffs' and Class Members' contact address data, photo metadata and fine geo-location coordinates, data generated not by the Hipster App, but sent by the Hipster App for offsite storage or processing. Defendant's App was acting as a virtual filing cabinet, and an offsite processor of data with respect to the data created. Defendant's App was functioning as either a filing cabinet or an advanced computer processing program that allows businesses to farm out sophisticated processing to a service that would process the information, with respect to the App geo-location data.

132. Heroku and Amazon EC2 servers were acting also as a "remote computing service," processing or storing Plaintiffs' and Class Members' contact address data, photos and/or photo's metadata, data sent to Heroku's and Amazon's EC2 servers by Defendant after obtaining such in an unauthorized manner.

133. Defendant intercepted Plaintiffs' Electronic Communications, transmitting in part, or whole, Plaintiffs' and Class Members' data to a Heroku and Amazon EC2 third-party cloud server. It is such access to the Heroku and Amazon EC2 servers where the unauthorized access to, and interception of Plaintiffs' and Class Members' data occurred. Defendant acquired Plaintiffs' and Class Members' Electronic Communications contemporaneously with transmission when it received the data as it was transmitted from Heroku and Amazon EC2, a third-party cloud server. Defendant had no authority to initially obtain Plaintiffs' and Class Members' contact address data, photo metadata, and/or fine GPS coordinates, no authority to then send such to Heroku and Amazon EC2, but it also had no authority to re-access such data on a systematic and continuous basis from such a remote computing service. Plaintiffs' and Class Members' data populating Heroku's and Amazon's EC2 servers should not have been re-accessed by Defendant, and once such occurred, Plaintiffs' and Class Members' Electronic Communications located on a Remote Computing Service was illegally accessed. Like any other entity that would have accessed Plaintiffs' and Class Members' data on Heroku and Amazon EC2 remote servers, Defendant had no right to access Plaintiffs' and Class Members' data on the Heroku and Amazon EC2 remote servers, even though Defendant had initially sent such data to Heroku's and Amazon's EC2 servers.

134. Discovery will be required to determine the extent of access to Plaintiffs' and Class Members' data by Heroku and Amazon and any associated third parties to determine whether the Defendant's contractual obligations with Amazon was regulated by category one, two or three noted above.

135. Plaintiffs will need discovery before being able to provide additional details about Defendant Hipster's App inner workings on Plaintiffs' and Class Members' mobile devices, inspection of Plaintiffs' and Class Members' data stored on Defendant's server's, and Heroku

and Amazon's EC2 servers, to ultimately prove the claims, made the basis of this action. Defendant's app utilizes highly advanced technology. It would be unrealistic and unjust for a court to require the Plaintiffs to provide precise, technical details concerning how their private, personal information was stored and transmitted. Nevertheless, the Complaint provides sufficient facts to draw a reasonable inference that the information accessed by Defendant was temporarily stored on Plaintiffs' computing mobile devices prior to transmission.

VI. PLAINTIFFS' EXPERIENCES

136. Plaintiffs Espitia, Zendejas and Fraire each store contact address data which contains information related to one (1) or more personal contacts, personal associations, business contacts, and professional contacts.

137. Plaintiffs Espitia, Zendejas and Fraire each downloaded and used Defendant's App during the Class Period;

138. Plaintiffs Espitia, Zendejas and Fraire each used their computing devices to access Defendant's app to use its services, including uploading and sharing digital content, such as photos.

139. Plaintiffs Espitia, Zendejas and Fraire each were subjected to the unauthorized access, use, dissemination, collection, and storage of personal information and information by Defendant.

140. Plaintiffs Espitia, Zendejas and Fraire were each unaware of the harm that would be imposed on them by Defendant, including use, retention and storage of their computing devices contact address data, installation of geo-tags for tracking, the misappropriation of their mobile device resources and bandwidth, as well the exploitation of their personal information.

141. None of the Plaintiffs Espitia, Zendejas and Fraire had knowledge that contact address book data was obtained and stored on Defendant's servers and/or third party cloud servers, and was obtained in an unreasonably insecure manner contrary to accepted standards – and in a way that is well-recognized to be easily accessible by even an unsophisticated hacker.

142. Plaintiffs Espitia, Zendejas and Fraire each had no knowledge, thus provide no consent to allowing Defendant access to their stored communications located on third party

servers, acting as a remote computing service.

143. None of the Plaintiffs Espitia, Zendejas and Fraire consented to having their data collected by Defendant. Had Plaintiffs known of Defendant's practices, they would not have downloaded its app. Plaintiffs were induced to download Defendant's app and the promise of a free safe, and reliable App; Defendant induced Plaintiffs to download its Hipster App by offering a service as a "free" App. However, Defendant failed to disclose to Plaintiffs that its "free" app would obtain and store their mobile device contact address book on it servers.

144. Each of the Plaintiffs Espitia, Zendejas and Fraire were not aware that Defendant would allow third parties to utilize Defendant-provided tools to collect Plaintiffs' information, without detection. For example, when Plaintiffs used the Defendant's app, its web analytic entities and ad networks routinely sent information about Plaintiffs to Defendant, and third parties that amassed and analyzed such data, receiving Plaintiffs' data which it used to uniquely identify and track Plaintiffs and Plaintiffs' contact without ever providing Plaintiffs a clue they were also being watched after leaving the Defendant's app platform, by Defendant and the mobile analytics company and ad networks; information transmitted through Defendant's app to third parties was transmitted in an unreasonably insecure manner—contrary to accepted standards—and in a way that is well-recognized to be easily intercepted by even an unsophisticated hacker sitting near a wireless hotspot.

145. None of the Plaintiffs ever authorized Defendant to cause such information to be shared with any third-party, advertising network or analytics provider, or be used for third party advertising purposes; considering their or her personal information to be private property and/or a confidential asset.

146. Plaintiffs Espitia, Zendejas and Fraire each had no means to avoid the data collection and tracking by Defendant and the third parties service: Defendant controls its ecosystem and what its App can and cannot transmit to third parties, and Defendant controls the fact that its customers are kept oblivious about the contact address book collection and storage process built into its ecosystem.

147. Plaintiffs Espitia, Zendejas and Fraire could not learn about the tracking

that goes on except through unreasonably burdensome efforts, such as those required in the investigations underlying these allegations, which are by no means comprehensive.

148. Defendant's act was based solely on commercial benefit. Defendant obtained revenue by marketing its ostensibly "free App," and the availability of its "free" Apps is tied to the availability of free data, including but not limited to the Plaintiffs' stored contact address data and data derived from non-Defendant members, by tracking Plaintiff, who had no idea what they was giving up, in terms of personal data, when they downloaded the app.

149. Plaintiffs' explicit privacy settings to the contrary, Defendant continues to track and store information about Plaintiffs, ignoring as a result that Plaintiffs could not prevent Defendant from collecting data. Defendant's representations to the contrary were false and/or misleading, and likely to deceive consumers targeted by such conduct.

150. Plaintiffs Espitia, Zendejas and Fraire each have standing to bring this case under Article III of the United States Constitution by virtue of alleging concrete, tangible and non-speculative injuries in fact, arising from violations of Federal statutes and the California Constitution. The statutes and Constitutional provisions at issue herein create legal rights, the invasion of which creates standing.

Standing of Plaintiffs and the Class

151. Plaintiffs and the Class Members are within the zone of persons sought to be protected by these statutory and Constitutional provisions, and if such parties cannot protect such interests and seek either remuneration or injunctive relief, they would have no mechanism available to hold Defendant accountable for such misconduct.

152. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of each Defendant's actions because Defendant accessed, used, disclosed, retained and stored their contact address book which contains confidential, and private personal data. Plaintiffs' personal data is property that was obtained by the Defendant without notice on authorization. Plaintiffs did not know, and Defendant did not have Plaintiffs' permission to access such data in the absence of Plaintiffs' and Class members' knowledge or

consent. Plaintiffs' personal property data and/or personal data assets include but are not limited to user's contact data, demographic information, geo-location information, and application usage habits.

153. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of Defendant's actions since Defendant used its services to install tracking mechanisms within Plaintiffs digital content. Plaintiffs shall be required to pay substantial sums to technical experts to review the digital content within their computing devices' memory to determine which digital content was accessed by Defendant's digital content functions in order to delete Defendant's tracking mechanisms.

154. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of each of Defendant's actions.

155. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of Defendant surreptitiously including in its App software certain code components that Plaintiffs would not reasonably have expected to be included, and which was installed on their devices without their permission, and which consumed portions of the "cache" and/or gigabytes of memory on their devices—memory that Plaintiffs paid for the exclusive use of when they purchased their mobile devices.

156. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of Defendant's conduct which has imposed undisclosed data transmittal costs on Plaintiffs.

157. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury to the security of Plaintiffs' person, and personally identifiable, information.

158. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of Defendant's conduct which has imposed imminent danger of physical harm by dissemination of a user's picture associated with their exact address, and as opposed to a coarse location, such as, for example, a picture of their home.

159. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury as a result of Defendant's conduct which has imposed risk of future identity

theft, by dissemination of a user's picture associated with their exact address, as opposed to coarse location.

160. Plaintiffs and similarly situated individuals have each suffered actual harm, economic injury, mental, and emotional distress as a result of each Defendant's conduct, by dissemination of a user's picture associated with their exact address, as opposed to coarse location, including but not limited to pictures of their home.

161. Plaintiffs and similarly situated individuals have each suffered actual harm and economic injury in that Defendant violated each individual Plaintiffs' legally protected privacy right to seclusion in their affairs by, in the aggregate, collecting Plaintiffs' personal information, to de-anonymize Plaintiffs and to personally identify them, their associations, and their activities with individuals offsite.

162. Plaintiffs and similarly situated individuals possess an ownership interest in their data that belongs to them and is subject to their control and alienability, and is a valuable commodity that has a property market value to advertisers. Plaintiffs thus have had property with an independent value taken from them by having it been taken beyond their control without compensation.

163. As such information was taken without their full knowledge or consent, and without Plaintiffs having obtained any compensation for the raw material taken from them, such a loss constitutes a classic Article III injury in terms of an uncompensated loss for which this Court can provide redress.

VII. CLASS ALLEGATIONS

164. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and 23(b)(3) on behalf of themselves and the following class:

> All persons residing in the United States that downloaded Defendant Hipster's App to their mobile computing devices from January 1, 2011 to the date of Class certification.

165. Excluded from the Class are Defendant, its legal representatives, assigns, and

successors, and any entity in which Defendant has a controlling interest. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

166. Plaintiffs reserve the right to revise this class definition based on facts they learn as litigation progresses.

167. The Class consists of thousands of individuals and other entities, making joinder impractical.

168. The claims of Plaintiffs are typical of the claims of all other Class Members.

169. Plaintiffs will fairly and adequately represent the interests of the other Class Members. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the Class Members, and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interests adverse to those of the other Class Members.

170. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and will have no effective remedy. The class treatment of common questions of law and fact is also superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

171. Defendant has acted, and failed to act, on grounds generally applicable to Plaintiffs and the other Class Members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members.

172. The factual and legal bases of Defendant's liability to Plaintiffs and to the other Class Members are the same, resulting in injury to Plaintiffs and all of the other Class Members. Plaintiffs and the other Class Members have all suffered harm and damages as a result of Defendant's wrongful conduct.

173. There are many questions of law and fact common to Plaintiffs and the Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not limited to the following:

a. whether Defendant's conduct described herein violates the Electronic Communications Privacy Act, 18 U.S.C. §2510

b. whether Defendant's conduct described herein violates the Stored Communications Act, 18 U.S.C. § 2701;

c. whether Defendant's conduct described herein violates California Computer Crime Law, Cal. Penal Code § 502;

d. whether Defendant's conduct described herein violates California's Invasion Of Privacy Act, California Penal Code § 630

e. whether Defendant's conduct described herein violates California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200;

f. whether Defendant's conduct described herein has violated State Consumer Protection Acts;

g. whether Defendant's conduct described herein has violated State Wiretap and Privacy Acts;

h. whether Defendant's conduct described herein has violated Bailment;

i. whether Defendant's conduct described herein has resulted in acts of Conversion;

j. whether Defendant's conduct described herein has resulted in an invasion of Privacy and Seclusion and Public Disclosure of Private Facts;

k. whether Defendant's conduct described herein has resulted in acts of Negligence;

l. whether Defendant's conduct described herein has resulted in Trespass to Personal Property/ Chattels; and

m. whether Defendant's conduct described herein has resulted in acts of Unjust Enrichment.

174. The questions of law and fact common to Class Members predominate over any questions affecting only individual members and a class action is superior to all other available

methods for the fair and efficient adjudication of this controversy.

COUNT I
Violations of the Electronic Communications Privacy Act,
18 U.S.C. §2510

175. Plaintiffs incorporate by reference and realleges all paragraphs previously alleged herein.

176. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

177. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, referred to as "ECPA," regulates wire and electronic communications interception and interception of oral communications, and makes it unlawful for a person to "willfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," within the meaning of 18 U.S.C. § 2511(1).

178. Defendant violated 18 U.S.C. § 2511 by intentionally acquiring and/or intercepting, by device or otherwise, Plaintiffs' and Class Members' electronic communications, without knowledge, consent, or authorization.

179. At all relevant times, Defendant engaged in business practices of intercepting Plaintiffs' and Class Members' electronic communications which included endeavoring to intercept the transmission of a user's contact address book and interactions between the user and its contact online from within their mobile device. Once the Defendant obtained the data they used such to aggregate mobile device data of the Plaintiffs and Class Members as they used their mobile device.

180. The contents of data transmissions from and to Plaintiffs' and Class Members' personal mobile device constitute "electronic communications" within the meaning of 18 U.S.C. §2510.

181. Plaintiffs are "person[s] whose … electronic communication is intercepted … or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520.

182. Defendant violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting,

endeavoring to intercept, or procuring any other person to intercept or endeavor to intercept Plaintiffs' electronic communications.

183. Defendant violated 18 U.S.C. § 2511(1)(c) by intentionally disclosing, or endeavoring to disclose, to any other person the contents of Plaintiffs' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' electronic communications.

184. Defendant violated 18 U.S.C. § 2511(1)(d) by intentionally using, or endeavoring to use, the contents of Plaintiffs' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' electronic communications.

185. Defendant's intentional interception of these electronic communications without Plaintiffs' or Class Members' knowledge, consent, or authorization was undertaken without a facially valid court order or certification.

186. Defendant intentionally used such electronic communications, with knowledge, or having reason to know, that the electronic communications were obtained through interception, for an unlawful purpose.

187. Defendant unlawfully accessed and used, and voluntarily disclosed, the contents of the intercepted communications to enhance their profitability and revenue through advertising. This disclosure was not necessary for the operation of Defendant's system or to protect Defendant's rights or property.

188. The Electronic Communications Privacy Act of 1986, 18 USC §2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used" in violation of the ECPA.

189. Defendant is liable directly and/or vicariously for this cause of action. Plaintiffs therefore seek remedy as provided for by 18 U.S.C. §2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and a reasonable

attorney's fee and other litigation costs reasonably incurred.

190. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

191. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendant's profits obtained from the above-described violations. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. § 2510.

COUNT II
Violations of the U.S. Stored Communications Act ("SCA"),
18 U.S.C. § 2701, et. seq.

192. Plaintiffs incorporate by reference and realleges all paragraphs previously alleged herein.

193. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

194. Pursuant to the Stored Communications Act ("SCA"), "electronic storage" means any "temporary storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2711(1); 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their recipient.

195. Congress enacted the SCA to prevent "unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public." Senate Report No. 99–541, S. REP. 99-541, 35, 1986 U.S.C.C.A.N. 3555, 3589.

196. As such, the SCA mandates, among other things, that it is unlawful for a person to obtain access to stored communications on another's computer system without authorization. 18

U.S.C. § 2701(a).

197. In violation of the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, Defendant intentionally accessed, without authorization, facilities through which electronic communications services were provided in that Defendant accessed Plaintiffs' and Class Members' contact address books, where such services and communications were restricted to access by Plaintiffs and Class Members, which Defendant obtained from Class Members through deception.

198. Defendant violated 18 U.S.C. § 2701(a)(1) by intentionally accessing its users' communications without authorization, and obtaining and/or altering authorized access to a wire or electronic communication while in electronic storage, within their mobile devices, by collecting contact address book data from Plaintiffs' and Class Members' mobile devices without authorization. In particular, Defendant intentionally bypassed user consent and obtained access to the contact address book data file located on the mobile devices that stores contact address book data. Defendant had actual knowledge of, and benefited from, this practice.

199. Defendant violated 18 U.S.C. § 2701(a)(2) by intentionally accessing its users' communications without authorization, and obtaining and/or altering authorized access to a wire or electronic communication while in electronic storage, within a provider of remote computing services, by collecting Plaintiffs' and Class Members' data without authorization. In particular, Defendant intentionally bypassed user consent and obtained access to data located on Heroku servers, a remote computing service. Defendant had actual knowledge of, and benefited from, this practice.

200. Defendant has violated 18 U.S.C. § 2701(a)(2) because it intentionally exceeded authorization to access users' communications and obtained, altered, or prevented authorized access to a wire or electronic communication while in electronic storage by collecting contact address book data from Plaintiffs' and the Class Members' mobile devices. Defendant had actual knowledge of, and benefited from, this practice.

201. Accordingly, Plaintiffs and Class Members are entitled to such equitable relief, civil damages, and punitive damages, and costs, and attorney's fees, as authorized under 18

U.S.C. § 2707.

COUNT III
Violations of Cal. Penal Code § 502,
The California Computer Crime Law ("CCCL")

202. Plaintiffs incorporate by reference the foregoing allegations.

203. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

204. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking, and using Plaintiffs' and the Class Members email address books.

205. Defendant accessed, copied, used, made use of, interfered with, and/or altered, data belonging to Class Members: (1) in and from the State of California; (2) in the home states of the Plaintiffs and the Class Members; and (3) in the states in which the servers that provided email services and communication links between Plaintiffs and Class Members and the websites with which they interacted were located.

206. Cal. Penal Code § 502(j) states: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

207. Defendant has violated California Penal Code § 502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiffs' email address books and using the contact information in the contact address books in order to execute a scheme to defraud consumers into registering as Defendant members and to wrongfully obtain the data in Plaintiffs' and the Class Members' email address books.

208. Defendant has violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' computers, computer system, and/or computer network.

209. Defendant has violated California Penal Code § 502(c)(7) by knowingly and

without permission accessing, or causing to be accessed, Plaintiffs' computer system, and/or computer network, in particular, their email services and data.

210. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" means any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.

211. Defendant has violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and the Class Members and Defendant, specifically, Defendant's App which propagates email address book harvesting computer instructions.

212. As a direct and proximate result of Defendant's unlawful conduct within the meaning of California Penal Code § 502, Defendant has caused loss to Plaintiffs and the Class Members in an amount to be proven at trial. Plaintiffs and the Class Members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

213. Plaintiffs and the Class Members seek compensatory damages, in an amount to be proven at trial, and injunctive or other equitable relief.

214. Plaintiffs and Class Members have suffered irreparable and incalculable harm and injuries from Defendant's violations. The harm will continue unless Defendant is enjoined from further violations of this section. Plaintiffs and Class Members have no adequate remedy at law.

215. Plaintiffs and the Class Members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because Defendant's violation were willful and, on information and belief, Defendant is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

216. Plaintiffs have also suffered irreparable injury from these unauthorized acts of disclosure, to wit: their personal, private, and sensitive communications have been harvested, viewed, accessed, stored, and used by Defendant, and have not been destroyed, and due to the continuing threat of such injury, have no adequate remedy at law, entitling Plaintiffs to injunctive relief.

COUNT IV
Violations of California's Invasion of Privacy Act,
California Penal Code § 630

217. Plaintiffs incorporate the above allegations by reference as if set forth herein at length.

218. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

219. Plaintiffs assert this claim against the California Defendant named herein in this complaint on behalf of themselves and the Class.

220. California Penal Code section 630 provides, in part:

> "Any person who, . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . ."

221. At all relevant times, Defendant's business practices of accessing the mobile device data of the Plaintiffs and Class Members was without authorization and consent; including, but not limited to, obtaining any and all communications.

222. On information and belief, Plaintiffs and Class Members, during one or more of their interactions on the Internet during the Class Period, communicated with one or more web entities based in California, or with one or more entities whose servers were located in California.

223. Communications from the California web-based entities to Plaintiffs and Class Members were sent from California. Communications to the California web-based entities from Plaintiffs and Class Members were sent to California.

224. Plaintiffs and Class Members did not consent to any of the Defendant's actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

225. Plaintiffs and Class Members did not consent to any of the Defendant's actions in

using the contents of their communications with such California-based entities.

226. Defendant is not a "public utility engaged in the business of providing communications services and facilities…"

227. The actions alleged herein by the Defendant were not undertaken: "for the purpose of construction, maintenance, conduct or operation of the services and facilities of the public utility."

228. The actions alleged herein by the Defendant were not undertaken with respect to any telephonic communication system used for communication exclusively within a state, county, city and county, or city correctional facility.

229. The Defendant directly participated in the interception, reading, and/or learning the contents of the communications between Plaintiffs, Class Members and California-based web entities.

230. Alternatively, and of equal violation of the California Invasion of Privacy Act, the Defendant aided, agreed with, and/or conspired with third parties to unlawfully do, or permit, or cause to be done all of the acts complained of herein.

231. Plaintiffs and Class Members have additionally suffered loss by reason of these violations, including, without limitation, violation of the right of privacy.

232. Unless restrained and enjoined, Defendant will continue to commit such acts. Pursuant to Section 637.2 of the California Penal Code, Plaintiffs and the class have been injured by the violations of California Penal Code section 631. Wherefore, Plaintiffs, on behalf of themselves and on behalf of a similarly situated Class of consumers, seek damages and injunctive relief.

COUNT V
Violations of California's Unfair Competition Law ("UCL"),
Cal. Business and Professions Code § 17200, et seq.

233. Plaintiffs incorporate by reference the foregoing allegations.

234. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

235. In violation of California Business and Professions Code § 17200 et seq., Defendant's conduct in this regard is ongoing and includes, but is not limited to, statements made by Defendant in its email messages regarding Defendant's possession of communications.

236. By engaging in the above-described acts and practices, Defendant has committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiffs and the Class have suffered injury-in-fact and have lost money and/or property.

237. Defendant's business acts and practices are unlawful, in part, because they violate California Business and Professions Code § 17500, et seq., which prohibits false advertising, in that they were untrue and misleading statements relating to Defendant's performance of services and with the intent to induce consumers to enter into obligations relating to such services, and regarding which statements Defendant knew or which, and by the exercise of reasonable care Defendant should have known, to be untrue and misleading. Defendant's business acts and practices are also unlawful in that they violate the California Consumer Legal Remedies Act, California Civil Code § 1750 et seq., Penal Code § 502, 18 U.S.C. § 1030, et. seq., and 18 U.S.C. § 2701, et. seq. Defendant is therefore in violation of the "unlawful" prong of the UCL.

238. Defendant's business acts and practices are unfair because they cause harm and injury in fact to Plaintiffs and Class Members and for which Defendant has no justification other than to increase, beyond what Defendant would have otherwise realized, its profit in fees from advertisers and its information assets through the acquisition of consumers' personal information. Defendant's conduct lacks reasonable and legitimate justification in that Defendant has benefited from such conduct and practices while Plaintiffs and the Class Members have been misled as to the nature and integrity of Defendant's services and have, in fact, suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendant's conduct offends public policy in California tethered to the Consumer Legal Remedies Act, the state constitutional right of privacy, and California statutes recognizing the need for consumers to obtain material information that enables them to safeguard their own privacy interests, including Cal. Civ. Code § 1798.80. In addition, Defendant's modus operandi constitutes a sharp practice in two ways: (i) Defendant know, or should know, that consumers

care about the status of personal information but are unlikely to be aware of the manner in which Defendant fails to fulfill its commitments to respect consumers' privacy; and (ii) to the extent members do become aware of Defendant's conduct and practices, Defendant's business model is designed to generate high traffic volume to make up for the loss of revenue from members disaffected by Defendant's misleading messages. Defendant is therefore in violation of the "unfair" prong of the UCL.

239. Defendant's acts and practices were fraudulent within the meaning of the UCL because they are likely to mislead the members of the public to whom they were directed.

240. Plaintiffs, on behalf of themselves and on behalf of each member of the Class, seek individual restitution, injunctive relief, and other relief allowed under the UCL.

COUNT VI
Breach of Bailment

241. Plaintiffs incorporate by reference and realleges all paragraphs previously alleged herein.

242. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

243. Plaintiffs and the Class each delivered to Defendants their digital media property.

244. Defendant owed a duty to exercise reasonable care to safeguard and protect Plaintiffs' and Class Members' digital media property. Defendant created a legal relationship that was binding, either expressly or impliedly, when it took actual possession of, or control over, Plaintiffs' and Class Members' property.

245. Defendant accepted consideration, by Plaintiffs' and Class Members' exchange of value when they relinquished the immediate right to control or possess the property.

246. Defendant, acting in deception, concealed its purpose to accept Plaintiffs and Class Member's digital media property, by accessing the metadata contained within photos uploaded by Plaintiffs and Class Members and/or photo's metadata taken by Plaintiffs and Class Members while accessing Defendant Hipster's App, in order to create a tracking mechanism, exceeding any permissions granted.

247. Defendant accessed, used, deleted, altered, or destroyed the photo metadata; acts which terminated the bailment, failing to return the property in the state it existed prior to the bailment.

248. Under Defendant's current "Terms," last accessed January 11, 2013, online: http://www.hipster.com/pages/terms -Defendant agreed to disclaim any ownership rights in Plaintiffs and the Class' property, and to hold and maintain the property for the exclusive benefit of Plaintiffs and the Class:

> "3. Subscriber Content
> Subscriber shall own all Subscriber Content that Subscriber contributes to the Site, but hereby grants and agrees to grant Hipster a non-exclusive, worldwide, royalty-free, transferable right and license (with the right to sublicense), to use, copy, cache, publish, display, distribute, modify, create derivative works and store such Subscriber Content and to allow others to do so ("Content License") in order to provide the Services."

249. The common law prohibits damage to property held in bailment. A bailment arises where possession, but not ownership, of property is transferred from one party ("bailor") to another ("bailee"). Where a bailee has received a bailment from a bailor, a duty of care is owed. Typically, a bailee is strictly liable for the bailment.

250. By engaging in the acts alleged in this complaint, without authorization or consent of Plaintiffs and Class Members, Defendant breached the bailment of Plaintiffs and Class Members digital content, referencing photos uploaded to, and/or taken by, Defendant Hipster's App.

251. As a result of Defendant's breach of this duty, Plaintiffs and all other Class Members have been harmed as alleged herein.

COUNT VII
Conversion

252. Plaintiffs hereby incorporate by reference the allegations contained in all of the preceding paragraphs of this complaint.

253. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

254. Plaintiffs and Class Members mobile device data, including, but not limited to,

their mobile devices' contact data, photo metadata, and GPS coordinates, are being used by Defendant to obtain sensitive and personal identifying information. Such property, owned by the Plaintiffs and Class Members, is valuable to the Plaintiffs and Class Members.

255. Plaintiffs and Class Members mobile devices' bandwidth was used by Defendant's activities, made the basis of this action, used without notice or authorization, for purposes not contemplated, not agreed to by Plaintiffs and Class Members when they downloaded Defendant Hipster's App. Such property, owned by the Plaintiffs and Class Members, is valuable to the Plaintiffs and Class Members.

256. Defendant unlawfully exercised dominion over said property and thereby converted Plaintiffs' and Class Members' property, by obtaining sensitive and personal identifying information, and by using Plaintiffs' and Class Members' bandwidth for data mining, in violation of collective Class Allegations, made the basis of this action.

257. Plaintiffs and Class Members were damaged thereby.

COUNT VIII
Invasion of Privacy and Seclusion and Public Disclosure of Private Facts

258. Plaintiffs incorporate by reference and realleges all paragraphs previously alleged herein.

259. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

260. The elements of the invasion of privacy tort of public disclosure of private facts are "(1) public disclosure (2) of a private fact (3) which would be offensive and objectionable to the reasonable person and (4) which is not of legitimate public concern." Shulman v. Group W Productions, Inc., 18 Cal. 4th 200 (1998). The elements of the invasion of privacy tort of intrusion into seclusion are "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." Id. at 231.

261. The private affairs of the Plaintiffs and Class Member include the contents of their private contact address books and contact information data stored on their mobile devices. This information is especially private and sensitive, because it reveals with whom the mobile

device user associates, identifies the mobile device owner's friends, business associates, and family, may contain contacts that the mobile device owner may not want publicly disclosed, sales leads, customer and client lists, and other similar information that reasonable people ordinarily understand to be private, especially when stored in their private contact address book on their mobile device.

262. Defendant's actions relating to Plaintiffs' and Class Members' private contact address book data, which were in violation of law and in flagrant contravention of contractual developer obligations, resulted in the taking and the public disclosure of such sensitive private information, as well as in intrusion into their private matters.

263. Plaintiffs' and the Class Members' private contact address book data is not a matter of legitimate public concern. Therefore, publicizing, disseminating, exposing or surreptitiously obtaining Plaintiffs' and Class Members' private contact address book data from their mobile devices is and will continue to be regarded as highly offensive and objectionable to reasonable people, especially where, as here, the commission of a crime (i.e., the illegal and unauthorized accessing of a computer and copying and use of its data) was necessary for Defendant to first acquire the contact address book data and learn their contents before their dissemination of the information.

264. Plaintiffs and the Class Members were, and continue to be, damaged as a direct and/or proximate result of Defendant's invasion of their privacy by the public disclosure of their private facts- the contents of their private contact address books from their mobile devices. Plaintiffs and the Class members are entitled to recover actual and nominal damages. Such damages include expenses for securing their mobile devices from another similar invasion of privacy, costs associated with re-securing the data and their mobile devices and computing devices, and procuring and verifying the removal, deletion and scrubbing of the data and data points from the Defendant's records, computers and systems, out of pocket expenses, and other economic and non- economic harm, for which they are entitled to compensation.

265. Defendant's wrongful actions constitute invasions of Plaintiffs' and Class Members' privacy by disturbing their seclusion and publicly disclosing their private facts

contained in their contact address books. As a direct and proximate result, Plaintiffs and the Class Members were harmed and suffered damages.

COUNT IX
Negligence

266. Plaintiffs incorporate by reference and realleges all paragraphs previously alleged herein.

267. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

268. Defendant owed a duty of care to Plaintiffs and Class Members.

269. Defendant came into possession of Plaintiffs' and Class Members' data and had a duty to exercise reasonable care in safeguarding and protecting such data.

270. Defendant failed to exercise reasonable care in safeguarding and protecting the data of Plaintiffs and Class Members.

271. Defendant breached such duty by negligently accessing, using, disseminating, storing, Plaintiffs' and Class Members' contact address data.

272. Defendant failed to fulfill its duty to Plaintiffs and Class Members, failing to fulfill even the minimum duty of care to protect Plaintiffs' and Class Members' personal information, privacy rights, security, and device resources.

273. Defendant breached their duty by negligently designing its Hipster App and permitting such to be uploaded to Plaintiffs' and Class Members' mobile devices, without any notice or authorization of its propensities, so that Defendant could acquire personal data without Plaintiffs' and Class Members' knowledge or permission.

302. Defendant also negligently made Plaintiffs' and Class Members' confidential data available to remote computing services in an unencrypted format. Defendant also negligently depleted Plaintiffs' and Class Members' mobile devices resources, including the unauthorized use of the resources of Plaintiffs' and Class Members' mobile devices' battery power, cell memory, CPUs, and bandwidth.

274. Plaintiffs and Class Members were harmed as a result of Defendant's breaches of its duty, and Defendant proximately caused such harms.

COUNT X
Trespass to Personal Property / Chattels

275. Plaintiffs incorporate by reference and reallege all paragraphs previously alleged herein.

276. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

277. The common law prohibits the intentional intermeddling with personal property, including a mobile device, in possession of another which results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property.

278. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiffs and Class Members, Defendant dispossessed Plaintiffs and Class Members from use and/or access to their mobile devices, or parts of them. Further, these acts impaired the use, value, and quality of Plaintiffs' and Class Members' mobile device. Defendant's acts constituted an intentional interference with the use and enjoyment of their mobile devices. By the acts described above, Defendant has repeatedly and persistently engaged in trespass to personal property in violation of the common law.

279. Without Plaintiffs' and Class Members' consent, or in excess of any consent given, Defendant knowingly and intentionally accessed Plaintiffs' and Class Members' property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property and causing injury to Plaintiffs and the members of the Class.

280. Defendant engaged in deception and concealment in order to gain access to Plaintiffs' and Class Members' mobile devices.

281. Defendant undertook the following actions with respect to Plaintiffs' and Class Members' mobile devices:

a) Defendant accessed and obtained control over the user's mobile device;

b) Defendant caused the installation of a new code onto the memory of the

user's mobile device;

c) Defendant programmed the operation of its code to function and operate without notice or consent on the part of the owner of the mobile device, and outside of the control of the owner of the mobile device.

282. All these acts described above were acts in excess of any authority any user granted when they downloaded Defendant Hipster's App and none of these acts was in furtherance of users viewing the Defendant Hipster App. By engaging in deception and misrepresentation, whatever authority or permission Plaintiffs and Class Members may have granted to Defendant was visited.

283. Defendant's installation and operation of its program used, interfered, and/or intermeddled with Plaintiffs' and Class Members' mobile devices. Such use, interference and/or intermeddling was without Class Members' consent or, in the alternative, in excess of Plaintiffs' and Class Members' consent.

284. Defendant's installation and operation of its program constitutes trespass, nuisance, and an interference with Class Members' chattels, to wit, their mobile device.

285. Defendant's installation and operation of its program impaired the condition and value of Class Members' mobile devices.

286. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiffs and Class Members.

287. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiffs' and Class Members' property, Defendant has injured and impaired in the condition and value of Class Members' computers, as follows:

a) By consuming the resources of and/or degrading the performance of Plaintiffs' and Class Members' mobile devices (including space, memory, processing cycles, and Internet connectivity);

b) By diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiffs' and Class Members' mobile devices;

c) By devaluing, interfering with, and/or diminishing Plaintiffs' and Class Members' possessory interest in their mobile devices;

d) By altering and controlling the functioning of Plaintiffs' and Class Members' mobile devices;

e) By infringing on Plaintiffs' and Class Members' right to exclude others from their mobile devices;

f) By infringing on Plaintiffs' and Class Members' right to determine, as owners of their mobile devices, which programs should be installed and operating on their mobile devices;

g) By compromising the integrity, security, and ownership of Class Members' mobile devices; and

h) By forcing Plaintiffs and Class Members to expend money, time, and resources in order to remove the program installed on their mobile devices without notice or consent.

COUNT XI
Common Law Counts of Unjust Enrichment Assumpsit, and Restitution

288. Plaintiffs incorporate by reference and realleges all paragraphs previously alleged herein.

289. Plaintiffs assert this claim against each and every Defendant named herein in this complaint on behalf of themselves and the Class.

290. Defendant entered into a series of implied at law contracts with Plaintiff.

291. Defendant engaged in conscious and deliberate conduct, that disappoints or frustrates Plaintiffs' reasonable privacy expectations that are implied in such agreements.

292. A benefit has been conferred upon Defendant by Plaintiffs and the Class. On information and belief, Defendant, directly or indirectly, has received and retained information regarding Plaintiffs' and Class Members' mobile device data that is otherwise private, confidential, and not of public record, and/or has received revenue from the use and provision of such information.

293. Defendant appreciates or has knowledge of said benefit.

294. Defendant has been unjustly enriched by the resulting profits enjoyed by Defendant as a result of such agreements. Plaintiffs' detriment and Defendant's enrichment were related to and flowed from the conduct challenged in this Complaint.

295. Under common law principles recognized in claims of common counts, unjust enrichment, restitution and/or assumpsit, Defendant should not be permitted to retain the benefits conferred upon them based on the taking of such data from Plaintiffs and Class Members and converting it into revenues and profits without providing compensation therefore.

296. Under principles of equity and good conscience, Defendant should not be permitted to retain the information and/or revenue that it acquired by virtue of its unlawful conduct. All funds, revenues, and benefits received by Defendant rightfully belong to Plaintiffs and the Class, which Defendant has unjustly received as a result of its actions.

297. Plaintiffs seek damages and restitutionary disgorgement of all profits or monies generated from such illegal acts, and the establishment of a constructive trust from which Plaintiffs may seek restitution as to all such funds, revenues and benefits that Defendant have unjustly received as a result of their actions that rightfully belong to Plaintiff.

298. California recognizes unjust enrichment as an independent cause of action. *See, e.g., Paracor Fin., Inc. v. Gen. Elec. Capital Corp.*, 96 F.3d 1151, 1167 (9th Cir. 1996) ("Under . . . California . . . law, unjust enrichment is an action in quasi-contract"). The holding in another recent ruling in the Northern District of California upheld a claim for unjust enrichment at this stage of the litigation. *In re Apple In-App Purchase Litig.*, No. 5:11-CV-1758 EJD, 2012 WL 1123548, at *9 (N.D. Cal. Mar. 31, 2012).

299. Plaintiffs also seek declaratory relief as to the rights and responsibilities of all parties to such implied-at-law agreements.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for the following relief:

a) With respect to all counts, declaring the action to be a proper class action and designating Plaintiffs and his counsel as representatives of the Class;

b) As applicable to the Class mutatis mutandis, awarding injunctive and equitable relief including, inter alia: (i) prohibiting Defendant from engaging in the acts alleged above; (ii) requiring Defendant to disgorge all of its ill-gotten gains to Plaintiffs and the other Class members, or to whomever the Court deems appropriate; (iii) requiring Defendant to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Defendant to provide Plaintiffs and the other Class Members a means to easily and permanently decline any participation in any data collection activities by means of Defendant or any similar online activity, in any present or future iteration of Defendant; (v) awarding Plaintiffs and Class Members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendant;

c) For a preliminary and permanent injunction restraining Defendant, its officers, agents, servants, employees, and attorneys, and those in active concert or participation with any of them from

    1) transmitting any information about Plaintiffs or Class Members' activities on the Internet for any purposes to any other websites or entities, without fair, clear and conspicuous notice of the intent to transmit information, including a full description of all information potentially and/or actually available for transmission;

    2) transmitting any information about Plaintiffs or Class Members' activities on the Internet for any purposes to any other websites or entities, without fair, clear and conspicuous opportunity to decline the transmittal prior to any transmission of data or information;

d) A permanent injunction enjoining and restraining Defendant, and all persons or entities acting in concert with them during the pendency of this action and thereafter perpetually, from:

1) initiating or procuring transmission of unsolicited commercial electronic messages on or through Class Members' computers, Class Members' email services and networks, or to Hipster users;
2) accessing or attempting to access Class Members' email services and networks, data, information, user information, profiles, computers and/or computer systems;
3) soliciting, requesting, or taking any action to induce Hipster visitors to provide identifying information, or representing that such solicitation, request, or action is being done with any Class Members' authorization or approval;
4) retaining any copies, electronic or otherwise, of any Class Members' information, including login information and/or passwords, obtained through illegitimate and/or unlawful actions;
5) engaging in any activity that alters, damages, deletes, destroys, disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Class Members' computers, computer systems, computer networks, data, websites, and email or other services;
6) engaging in any unlawful activities alleged in this complaint; and
7) entering or accessing any of the physical premises or facilities of Class Members or their counsel.

e) An award to Class Members of damages, including, but not limited to, compensatory, statutory, exemplary, aggravated, and punitive damages, as permitted by law and in such amounts to be proven at trial;

f) An award to Class Members of reasonable costs, including reasonable attorneys' fees;

g) For pre-and post-judgment interest as allowed by law; and

h) For such other relief as the Court may deem just and proper.

Dated: January 30, 2013

Respectfully submitted,

By:_____
DAVID C. PARISI
One of the Attorneys for Plaintiff, individually and on behalf of Class of similarly situated individuals

David C. Parisi, Esq. (162248)
dparisi@parisihavens.com
Suzanne Havens Beckman, Esq. (188814)
shavens@parisihavens.com
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, CA 91403
Telephone: (818) 990-1299

Alan Himmelfarb (90480)
The Law Offices of Alan Himmelfarb
80 W. Sierra Madre Blvd., # 304
Sierra Madre, CA 91024
Telephone: (626) 325-3104
consumerlaw1@earthlink.net

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100

JURY DEMAND

Plaintiffs request trial by jury of all claims that can be so tried.

Dated: January 30, 2013

Respectfully submitted,

By: _____
DAVID C. PARISI
One of the Attorneys for Plaintiff, individually and on behalf of Class of similarly situated individuals

David C. Parisi, Esq. (162248)
dparisi@parisihavens.com
Suzanne Havens Beckman, Esq. (188814)
shavens@parisihavens.com
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, CA 91403
Telephone: (818) 990-1299

Alan Himmelfarb (90480)
The Law Offices of Alan Himmelfarb
80 W. Sierra Madre Blvd., # 304
Sierra Madre, CA 91024
Telephone: (626) 325-3104
consumerlaw1@earthlink.net

Joseph H. Malley (not admitted)
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, TX 75208
Telephone: (214) 943-6100