

1 HEDIN HALL LLP
Frank S. Hedin (SBN 291289)
2 fhedin@hedinhall.com
Four Embarcadero Center, Suite 1400
3 San Francisco, California 94104
Telephone: (415) 766-3534
4 Facsimile: (415) 402-0058

5 AHDOOT & WOLFSON, PC
Robert Ahdoot (SBN 172098)
6 rahdoot@ahdootwolfson.com
10728 Lindbrook Drive
7 Los Angeles, California 90024
Telephone: (310) 474-9111
8 Facsimile: (310) 474-8585

9 BURSOR & FISHER, P.A.
L. Timothy Fisher (SBN 191626)
10 ltfisher@bursor.com
1990 North California Blvd., 940
11 Walnut Creek, California 94596
Telephone: (925) 300-4455
12 Facsimile: (925) 407-2700

13 [Additional counsel on signature page]

14 *Counsel for Plaintiffs and the Putative Classes*

15 **UNITED STATES DISTRICT COURT**
16 **NORTHERN DISTRICT OF CALIFORNIA**

18 LEIGH WHEATON; JILL PAUL; and
TREVOR PAUL, individually and on behalf
19 of all others similarly situated,

20 Plaintiffs,

21 v.

22 APPLE INC.,

23 Defendant.

Case No. _____

CLASS ACTION

CLASS ACTION COMPLAINT

1 On behalf of themselves and all others similarly situated, Plaintiffs Leigh
2 Wheaton, Jill Paul, and Trevor Paul complain and allege as follows based on personal
3 knowledge as to themselves, the investigation of their counsel, and information and
4 belief as to all other matters, and demand trial by jury. Plaintiffs believe that substantial
5 evidentiary support will exist for the allegations in this complaint, after a reasonable
6 opportunity for discovery.

7 **NATURE OF THE CASE**

8 1. In early 2019, in an effort to capitalize on recent revelations concerning
9 the data-sharing practices of its competitors Facebook, Inc. and Google LLC, Apple
10 Inc. (“Apple”) placed a massive billboard in Las Vegas, Nevada touting its supposedly
11 pro-consumer positions on issues of data privacy:



21 2. The statement on the billboard is plainly untrue, however, because – as
22 will be explained in detail below – none of the information pertaining to the music you
23 purchase on your iPhone stays on your iPhone.

24

1 3. To supplement its revenues and enhance the formidability of its brand in
2 the eyes of mobile application developers, Apple sells, rents, transmits, and/or
3 otherwise discloses, to various third parties, information reflecting the music that its
4 customers purchase from the iTunes Store application that comes pre-installed on their
5 iPhones. The data Apple discloses includes the full names and home addresses of its
6 customers, together with the genres and, in some cases, the specific titles of the
7 digitally-recorded music that its customers have purchased via the iTunes Store and
8 then stored in their devices' Apple Music libraries (collectively "Personal Listening
9 Information"). After Apple discloses its customers' Personal Listening Information,
10 the various third-party recipients of this data then append to it a myriad of other
11 categories of personal information pertaining to Apple's customers – such as gender,
12 age, household income, educational background, and marital status – only to then re-
13 sell that Personal Listening Information (enhanced with various categories of
14 demographic data) to other third parties on the open market.

15 4. Rhode Island resident Leigh Wheaton brings this action for legal and
16 equitable remedies to redress and put a stop to the illegal actions of Apple in disclosing
17 to third parties her Personal Listening Information and that of all other similarly-
18 situated Rhode Island residents who purchased music from Apple on its iTunes Store
19 platform, in violation of Rhode Island's Video, Audio and Publication Rentals Privacy
20 Act, R.I. Gen. Laws § 11-18-32 (the "RIVRPA").

21 5. Additionally, Michigan residents Jill Paul and Trevor Paul, individually
22 and on behalf of all others similarly situated, bring this action for legal remedies to
23 redress the illegal actions of Apple in disclosing to third parties, between May 24, 2016
24

1 and July 30, 2016, their Personal Listening Information and that of all other similarly-
2 situated Michigan residents who purchased music from Apple on its iTunes Store
3 platform, in violation of Michigan’s Preservation of Personal Privacy Act, H.B. 5331,
4 84th Leg., Reg. Sess., P.A. No. 378, §§ 1-4 (Mich. 1988), *id.* § 5, added by H.B. 4694,
5 85th Leg., Reg. Sess., P.A. No. 206, § 1 (Mich. 1989) (the “MIPPPA”).¹

6 6. As set forth below, Apple has sold, rented, transmitted, and/or otherwise
7 disclosed the Personal Listening Information of the Plaintiffs and millions of its other
8 customers to developers of various mobile applications available for download in its
9 App Store, as well as to data aggregators, data appenders, data cooperatives, list
10 brokers, and other third parties, many of whom have in turn re-disclosed Plaintiffs’ and
11 the other unnamed class members’ Personal Listening Information to other third parties
12 for further exploitation and monetization – all without providing prior notice to or
13 obtaining the requisite consent from anyone. Such disclosures invaded Plaintiffs’ and
14 the unnamed Class members’ privacy and have resulted in a barrage of unwanted junk
15 mail to their home addresses and e-mail inboxes.

16 7. The Rhode Island RIVRPA and the Michigan MIPPPA clearly prohibit
17 what Apple has done. Subsection (a) of Rhode Island’s RIVRPA provides:

18 _____
19 ¹ In May 2016, the Michigan legislature amended the MIPPPA. *See* S.B. 490, 98th
20 Leg., Reg. Sess., P.A. No. 92 (Mich. 2016) (codified at M.C.L. § 445.1711, *et seq.*).
21 The May 2016 amendment to the MIPPPA, which became effective on July 31, 2016,
22 does not apply retroactively to claims that accrued prior to its July 31, 2016 effective
23 date. *See Boelter v. Hearst Commc’ns, Inc.*, 192 F. Supp. 3d 427, 439-41 (S.D.N.Y.
24 2016) (holding that “the amendment to the [MIPP]PA does not apply to Plaintiffs’
claims, and the Court will assess the sufficiency of those claims under the law as it was
when Plaintiffs’ claims accrued.”) (citing *Landgraf v. USI Film Prods.*, 511 U.S. 224,
286 (1994)). Because the claims alleged herein accrued, and thus vested, prior to the
July 31, 2016 effective date of the amended version of the MIPPPA, the unamended
version of the MIPPPA applies in this case. *See Horton v. GameStop, Corp.*, No. 18-
cv-00596-GJQ-PJG, Dkt. 18 at 3-5 (W.D. Mich. 2018).

1 It shall be unlawful for any person to reveal, transmit,
2 publish, or disseminate in any manner, any records which
3 would identify the names and addresses of individuals, with
4 the titles or nature of video films, records, cassettes, or the
5 like, which they purchased, leased, rented, or borrowed, from
6 libraries, book stores, video stores, or record and cassette
7 shops or any retailer or distributor of those products, whether
8 or not the identities and listings are kept in a remote
9 computing service or electronic storage or the disclosure is
10 made through or by a remote computing service.

11 RIVRPA § (a) (emphasis added). Similarly, section 2 of the MIPPPA provides:

12 [A] person, or an employee or agent of the person, engaged
13 in the business of selling at retail, renting, or lending books
14 or other written materials, sound recordings, or video
15 recordings shall not disclose to any person, other than the
16 customer, a record or information concerning the purchase,
17 lease, rental, or borrowing of those materials by a customer
18 that indicates the identity of the customer.

19 MIPPPA § 2 (emphasis added).

20 8. Thus, while Apple profits handsomely from its unauthorized sale, rental,
21 transmission, and/or disclosure of its customers' Personal Listening Information, it
22 does so at the expense of its customers' privacy and statutory rights because Apple
23 does not notify let alone obtain the requisite written consent from its customers prior
24 to disclosing their Personal Listening Information.

8. Apple's disclosures of the Personal Listening Information of Plaintiffs and
the other unnamed Class members were not only unlawful, they were also dangerous
because such disclosures allow for the targeting of particularly vulnerable members of
society. For example, any person or entity could rent a list with the names and
addresses of all unmarried, college-educated women over the age of 70 with a
household income of over \$80,000 who purchased country music from Apple via its
iTunes Store mobile application. Such a list is available for sale for approximately \$136
per thousand customers listed.

1 has regularly purchased digital music, including rock music, from Apple via Apple’s
2 iTunes Store, using his iPhone.

3 16. Defendant Apple Inc. is a Delaware corporation with its principal place of
4 business in Cupertino, California. Apple does business throughout California and
5 across the United States. Apple is a retailer and distributor of digital music, which it
6 sells to consumers online via its iTunes Store mobile application.

7 **APPLICABLE STATUTORY SCHEMES**

8 17. In 1988, leading up to the enactment of the federal Video Privacy
9 Protection Act (“VPPA”), 18 U.S.C. § 2710, members of the United States Senate
10 warned that records of consumers’ purchases and rentals of audiovisual and publication
11 materials offer “a window into our loves, likes, and dislikes,” and that “the trail of
12 information generated by every transaction that is now recorded and stored in
13 sophisticated record-keeping systems is a new, more subtle and pervasive form of
14 surveillance.” S. Rep. No. 100-599 at 7-8 (1988) (statements of Sens. Simon and
15 Leahy, respectively).

16 18. As Senator Patrick Leahy recognized in proposing the Video and Library
17 Privacy Protection Act (later codified as the VPPA), “[i]n practical terms our right to
18 privacy protects the choice of movies that we watch with our family in our own homes.
19 And it protects the selection of books that we choose to read.” 134 Cong. Rec. S5399
20 (May 10, 1988). The personal nature of such information, and the need to protect it
21 from disclosure, is the *raison d’être* of the statute: “These activities are at the core of
22 any definition of personhood. They reveal our likes and dislikes, our interests and our
23
24

1 whims. They say a great deal about our dreams and ambitions, our fears and our hopes.
2 They reflect our individuality, and they describe us as people.” *Id.*

3 19. Following the VPPA’s enactment, several states, including Rhode Island
4 and Michigan, quickly followed suit.

5 **I. Rhode Island’s Video, Audio, And Publication Rentals Privacy Act**

6 20. Recognizing the need to further protect its citizens’ privacy rights, Rhode
7 Island’s legislature enacted the RIVRPA to “prohibit[] the revealing of records relating
8 to the rental of video or audio tapes or publications.” Explanation By The Legislat
9 Council, attached as **Exhibit A**.

10 21. Subsection (a) of the RIVRPA states:

11 It shall be unlawful for any person to reveal, transmit,
12 publish, or disseminate in any manner, any records which
13 would identify the names and addresses of individuals, with
14 the titles or nature of video films, records, cassettes, or the
15 like, which they purchased, leased, rented, or borrowed, from
16 libraries, book stores, video stores, or record and cassette
17 shops or any retailer or distributor of those products, whether
18 or not the identities and listings are kept in a remote
19 computing service or electronic storage or the disclosure is
20 made through or by a remote computing service.

21 RIVRPA § (a) (emphasis added).

22 22. Despite the fact that tens of thousands of Rhode Island residents have
23 purchased music from Apple via its iTunes Store platform, Apple has disregarded its
24 legal responsibilities to these individuals by systematically disclosing their Personal
Listening Information in violation of the RIVRPA.

25 **II. Michigan’s Personal Privacy Preservation Act**

26 23. Also recognizing the need to further protect its citizens’ privacy rights,
Michigan’s legislature enacted the MIPPPA “to preserve personal privacy with respect

1 to the purchase, rental, or borrowing of certain [audiovisual and reading] materials,” by
2 prohibiting companies from disclosing certain types of sensitive consumer information
3 pertaining thereto. H.B. No. 5331, 1988 Mich. Legis. Serv. 378 (West).

4 24. Subsection 2 of the MIPPPA states:

5 [A] person, or an employee or agent of the person, engaged
6 in the business of selling at retail, renting, or lending books
7 or other written materials, sound recordings, or video
8 recordings shall not disclose to any person, other than the
customer, a record or information concerning the purchase,
lease, rental, or borrowing of those materials by a customer
that indicates the identity of the customer.

9 MIPPPA § 2 (emphasis added).

10 25. Michigan’s passage of the MIPPPA also established as a matter of law
11 “that a person’s choice in reading, music, and video entertainment is a private matter,
12 and not a fit subject for consideration by gossipy publications, employers, clubs, or
13 anyone else for that matter.” *Privacy: Sales, Rentals of Videos, etc.*, House Legislative
14 Analysis Section, H.B. No. 5331, Jan. 20, 1989 (attached hereto as **Exhibit B**).

15 26. Despite the fact that hundreds of thousands of Michigan residents have
16 purchased music from Apple via its iTunes Store platform, Apple has disregarded its
17 legal responsibilities to these individuals by systematically disclosing their Personal
18 Listening Information in violation of the MIPPPA.

19 **BACKGROUND FACTS**

20 **I. Consumers’ Personal Information Has Real Market Value**

21 27. In 2001, Federal Trade Commission (“FTC”) Commissioner Orson
22 Swindle remarked that “the digital revolution . . . has given an enormous capacity to
23 the acts of collecting and transmitting and flowing of information, unlike anything
24

1 we've ever seen in our lifetimes . . . [and] individuals are concerned about being defined
2 by the existing data on themselves.”²

3 28. More than a decade later, Commissioner Swindle’s comments ring truer
4 than ever, as consumer data feeds an information marketplace that supports a \$26
5 billion dollar per year online advertising industry in the United States.³

6 29. The FTC has also recognized that consumer data possesses inherent
7 monetary value within the new information marketplace and publicly stated that:

8 Most consumers cannot begin to comprehend the types and
9 amount of information collected by businesses, or why their
10 information may be commercially valuable. Data is currency.
The larger the data set, the greater potential for analysis – and
profit.⁴

11 30. In fact, an entire industry exists while companies known as data
12 aggregators purchase, trade, and collect massive databases of information about
13 consumers. Data aggregators then profit by selling this “extraordinarily intrusive”
14 information in an open and largely unregulated market.⁵

16 ² FCC, *The Information Marketplace* (Mar. 13, 2001), at 8-11, available at
17 [https://www.ftc.gov/sites/default/files/documents/public_events/information-
marketplace-merging-and-exchanging-consumer-data/transcript.pdf](https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf).

18 ³ See *Web’s Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011),
19 [http://online.wsj.com/article/SB10001424052748703529004576160764037920274.ht
ml](http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html) (last visited May 13, 2019).

20 ⁴ Statement of FTC Cmr. Harbour (Dec. 7, 2009), at 2, available at
21 [https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-
exploring-privacy-roundtable/091207privacyroundtable.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf).

22 ⁵ See M. White, *Big Data Knows What You’re Doing Right Now*, TIME.com (July
23 31, 2012), [http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-
right-now/](http://moneyland.time.com/2012/07/31/big-data-knows-what-youre-doing-right-now/) (last visited May 13, 2019).

1 31. The scope of data aggregators’ knowledge about consumers is immense:
2 “If you are an American adult, the odds are that [they] know[] things like your age,
3 race, sex, weight, height, marital status, education level, politics, buying habits,
4 household health worries, vacation dreams—and on and on.”⁶

5 32. Further, “[a]s use of the Internet has grown, the data broker industry has
6 already evolved to take advantage of the increasingly specific pieces of information
7 about consumers that are now available.”⁷

8 33. Recognizing the serious threat the data mining industry poses to
9 consumers’ privacy, on July 25, 2012, the co-Chairmen of the Congressional Bi-
10 Partisan Privacy Caucus sent a letter to nine major data brokerage companies seeking
11 information on how those companies collect, store, and sell their massive collections
12 of consumer data, stating in pertinent part:

13 By combining data from numerous offline and online
14 sources, data brokers have developed hidden dossiers on
15 every U.S. consumer. This large[-]scale aggregation of the
personal information of hundreds of millions of American
citizens raises a number of serious privacy concerns.⁸

16
17 ⁶ N. Singer, *You for Sale: Mapping, and Sharing, the Consumer Genome*, N.Y.
Times (June 16, 2012), available at
18 [http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-
consumer-database-marketing.html](http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html) (last visited May 13, 2019).

19 ⁷ Letter from Sen. J. Rockefeller IV, Sen. Cmtee. on Commerce, Science, and
20 Transportation, to S. Howe, Chief Executive Officer, Acxiom (Oct. 9, 2012) available
at [http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-
4157-a97b-a658c3c3061c](http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=3bb94703-5ac8-4157-a97b-a658c3c3061c).

21
22 ⁸ See *Bipartisan Group of Lawmakers Query Data Brokers About Practices*
23 *Involving Consumers’ Personal Information*, Website of Sen. Markey (July 24, 2012),
[http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-
query-data-brokers-about-practices-involving-consumers-personal-information](http://www.markey.senate.gov/news/press-releases/bipartisan-group-of-lawmakers-query-data-brokers-about-practices-involving-consumers-personal-information).

1 34. Data aggregation is especially troublesome when consumer information
2 is sold to direct-mail advertisers. In addition to causing waste and inconvenience,
3 direct-mail advertisers often use consumer information to lure unsuspecting consumers
4 into various scams,⁹ including fraudulent sweepstakes, charities, and buying clubs.
5 Thus, when companies like Apple share information with data aggregators, data
6 cooperatives, and direct-mail advertisers, they contribute to the “[v]ast databases of
7 names and personal information” that are often “sold to thieves by large publicly traded
8 companies,” which “put[s] almost anyone within the reach of fraudulent telemarketers”
9 and other criminals.¹⁰

10 35. Disclosures like Apple’s are particularly dangerous to the elderly. “Older
11 Americans are perfect telemarketing customers, analysts say, because they are often at
12 home, rely on delivery services, and are lonely for the companionship that telephone
13 callers provide.”¹¹ The FTC notes that “[t]he elderly often are the deliberate targets of
14 fraudulent telemarketers who take advantage of the fact that many older people have
15 cash reserves or other assets to spend on seemingly attractive offers.”¹²

16
17
18 ⁹ See *Prize Scams*, Federal Trade Commission, <http://www.consumer.ftc.gov/articles/0199-prize-scams> (last visited May 13, 2019).

19 ¹⁰ C. Duhigg, *Bilking the Elderly, With a Corporate Assist*, N.Y. Times (May 20,
20 2007), available at <http://www.nytimes.com/2007/05/20/business/20tele.html> (last
21 visited May 13, 2019).

22 ¹¹ *Id.*

23 ¹² *Fraud Against Seniors: Hearing before the Senate Special Committee on Aging*
24 (August 10, 2000) (prepared statement of the FTC), available at https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-fraud-against-seniors/agingtestimony.pdf.

1 36. Indeed, an entire black market exists where the personal information of
2 vulnerable elderly Americans is exchanged. Thus, information disclosures like Apple’s
3 are particularly troublesome because of their cascading nature: “Once marked as
4 receptive to [a specific] type of spam, a consumer is often bombarded with similar
5 fraudulent offers from a host of scam artists.”¹³

6 37. Apple is not alone in jeopardizing its subscribers’ privacy and well-being
7 in exchange for increased revenue: disclosing subscriber information to data
8 aggregators, data appenders, data cooperatives, direct marketers, and other third parties
9 is a widespread practice in the publishing industry.

10 38. Thus, as consumer data has become an ever-more valuable commodity,
11 the data mining industry has experienced rapid and massive growth. Unfortunately for
12 consumers, this growth has come at the expense of their most basic privacy rights.

13 **II. Consumers Place Monetary Value on their Privacy and Consider** 14 **Privacy Practices When Making Purchases**

15 39. As the data aggregation and cooperative industry has grown, so too have
16 consumer concerns regarding the privacy of their personal information.

17 40. A recent survey conducted by Harris Interactive on behalf of TRUSTe,
18 Inc. showed that 89 percent of consumers polled avoid doing business with companies
19 who they believe do not protect their privacy online.¹⁴ As a result, 81 percent of

20
21 ¹³ *Id.*

22 ¹⁴ See 2014 TRUSTe US Consumer Confidence Privacy Report, TRUSTe,
23 [http://www.theagitator.net/wp-](http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf)
24 [content/uploads/012714_ConsumerConfidenceReport_US1.pdf](http://www.theagitator.net/wp-content/uploads/012714_ConsumerConfidenceReport_US1.pdf) (last visited May 13,
2019).

1 smartphone users polled said that they avoid using smartphone apps that they don't
2 believe protect their privacy online.¹⁵

3 41. Thus, as consumer privacy concerns grow, consumers are increasingly
4 incorporating privacy concerns and values into their purchasing decisions and
5 companies viewed as having weaker privacy protections are forced to offer greater
6 value elsewhere (through better quality and/or lower prices) than their privacy-
7 protective competitors.

8 42. In fact, consumers' personal information has become such a valuable
9 commodity that companies are beginning to offer individuals the opportunity to sell
10 their personal information themselves.¹⁶

11 43. These companies' business models capitalize on a fundamental tenet
12 underlying the personal information marketplace: consumers recognize the economic
13 value of their private data. Research shows that consumers are willing to pay a
14 premium to purchase services from companies that adhere to more stringent policies of
15 protecting their personal data.¹⁷

16
17 ¹⁵ *Id.*

18 ¹⁶ See Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal*
19 *Data*, N.Y. Times (Feb. 12, 2012), available at
20 <http://www.nytimes.com/2012/02/13/technology/start-ups-aim-to-help-users-put-a-price-on-their-personal-data.html> (last visited May 13, 2019).

21 ¹⁷ See Tsai, Cranor, Acquisti, and Egelman, *The Effect of Online Privacy*
22 *Information on Purchasing Behavior*, 22(2) Information Systems Research 254, 254
23 (2011); see also European Network and Information Security Agency, *Study on*
24 *monetising privacy* (Feb. 27, 2012), available at
<https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/monetising-privacy> (last visited May 13, 2019).

1 44. Thus, in today’s digital economy, individuals and businesses alike place a
2 real, quantifiable value on consumer data and corresponding privacy rights.¹⁸ As such,
3 while a business offers customers a service that includes statutorily guaranteed privacy
4 protections, yet fails to honor these guarantees, the customer receives a service of less
5 value than the service paid for.

6 **III. Apple Unlawfully Sells, Rents, Transmits, And Otherwise Discloses Its** 7 **Customers’ Personal Listening Information**

8 45. Apple maintains a vast digital database comprised of all of its customers’
9 Personal Listening Information, including information reflecting the genres and titles
10 of all digital music sold to its customers via its iTunes Store platform.¹⁹

11 46. During the time period relevant to this action, Apple has monetized this
12 data in at least two primary ways: (1) by selling, renting, transmitting and/or otherwise
13 disclosing lists comprised of its customers’ Personal Listening Information and other
14 highly-personalized demographic information to various third parties; and (2)
15 transmitting and disclosing its customers’ full iTunes libraries, comprised of such
16 detailed Personal Listening Information as the specific titles of the songs and albums

17 ¹⁸ See Hann, et al., *The Value of Online Information Privacy: An Empirical*
18 *Investigation* (Oct. 2003) at 2, available at
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.321.6125&rep=rep1&type=pdf> (last visited May 13, 2019) (“It is obvious that people value online privacy.”).

19 ¹⁹ See also Titlow, John Paul, *iTunes Radio: Smart for Apple, “Meh” for Users,*
20 *And Harmless for Pandora*, Sept. 18, 2013, available at
21 [https://www.fastcompany.com/3017612/itunes-radio-smart-for-apple-meh-for-users-](https://www.fastcompany.com/3017612/itunes-radio-smart-for-apple-meh-for-users-and-harmless-for-pandora)
22 [and-harmless-for-pandora](https://www.fastcompany.com/3017612/itunes-radio-smart-for-apple-meh-for-users-and-harmless-for-pandora) (last visited May 13, 2019) (reporting that Apple was using
23 various music-purchasing and listening applications to “collect[] new data points in
24 the form of users tapping those thumb buttons, not to mention skipping, or most
tellingly of all, purchasing songs and albums. Over time, these insights will
strengthen Apple’s music recommendation engine, which is presumably already
pry to the day-to-day listening habits of hundreds of millions of users.”) (emphasis
added).

1 that its customers have purchased, to various iOS mobile application developers, who
2 in turn have further disclosed this detailed Personal Listening Information to data
3 brokers, data miners, mobile application developers, marketers, and other third parties.

4 **A. Apple Sells Mailing Lists Comprised of its Customers’ Personal**
5 **Listening Information to Anyone Willing to Pay**

6 47. First, Apple discloses its customers’ Personal Listening Information,
7 identifying the names and addresses of its customers and the particular genres of music
8 they have purchased from its iTunes Store, to data aggregators, data miners, data
9 brokers, data appenders, and other third parties, who then supplement that information
10 with additional sensitive personal information about each of Apple customers,
11 including their age, gender, purchasing habits, education, household income, and
12 (when applicable) the number, age, and gender of the subscriber’s children.

13 48. These factual allegations are corroborated by publicly-available evidence.
14 For instance, as shown in the screenshot below, the Personal Listening Information of
15 18,188,721 “iTunes and Pandora Music Purchasers,” residing across the United States
16 (including in Michigan and Rhode Island), is offered for sale on the website of Carney
17 Direct Marketing (“CDM”) – one of many traffickers of this type of Personal Listening
18 Information – at a base price of “\$80/M [per thousand records]” (8 cents each):
19
20
21
22
23
24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

SEGMENTS	PRICE	ID NUMBER
18,188,721 TOTAL UNIVERSE / BASE RATE	\$80.00/M	NextMark 385690
1 Month Hotline	+ \$12.00/M	Manager
3 Month Hotline	+ \$8.00/M	UNIVERSE
		18,188,721
		LIST TYPE
		Consumer 
DESCRIPTION		SOURCE
iTunes and Pandora music Purchasers are consumers using major internet providers for their music listening pleasure. iTunes and Pandora Music Purchasers enjoy playing their favorite radio stations from home, work, or mobile devices. Individual song, video and record purchases and/or commercial free listening allow for a highly custom playlist along with a much wider geographical reach than local radio stations for a higher quality transmitted sound. These purchasers get access to more stations and a wider variety of programming options all hand selected by the individual.		LIST MAINTENANCE
		Counts through 04/01/2019
		Last update 04/01/2019
		Next update 05/01/2019
		SELECTS
		AGE 10.00/M
		Buying Behavior
		Demographic
		Education 8.00/M
		Full Lifestyle
		GENDER 10.00/M
		Geography 8.00/M
		House Hold Income 10.00/M
		Interest
		Mail Order Buyer 10.00/M
		MARITAL STATUS 10.00/M
		PRESENCE OF CHILDREN 10.00/M
		GEOGRAPHY
		USA

See **Exhibit C** hereto.

49. The “iTunes and Pandora Music Purchasers” list offered for sale by CDM contains the Personal Listening Information of tens of thousands of Rhode Island residents and hundreds of thousands of Michigan residents who have purchased music from Apple’s iTunes Store. The “iTunes and Pandora Music Purchasers” list includes, for each Rhode Island and Michigan purchaser of music appearing on the list, the person’s name and address, “age,” “house hold income,” “education,” “gender,” “geography,” “presence of children” and, significantly, “buying behavior,” which identifies the particular genre(s) of music that the person purchased from Apple.

1 50. SRDS, another list brokerage company, offers for sale the same or a
 2 similar list as the one sold by CDM, at the same price, and additionally offers a finder's
 3 fee to brokers who are able to find purchasers of this Personal Listening Information
 4 (offering "20% commission to brokers" and "15% commission to agencies"), as shown
 5 in the screenshot below of a publicly-accessible webpage on SRDS's website:

6

7

8

9

10

11

12

13

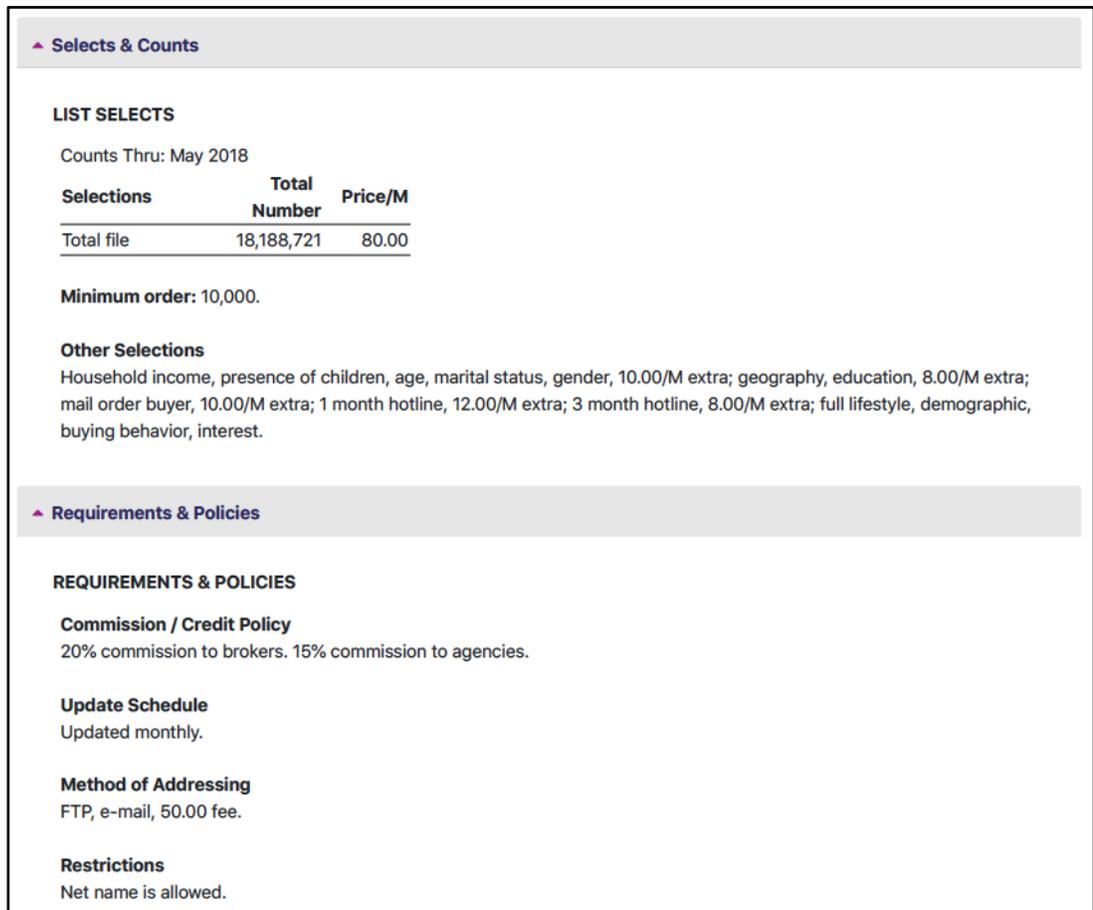
14

15

16

17

18



The screenshot displays a webpage section titled "Selects & Counts" with a sub-section "LIST SELECTS". It includes a table with columns for "Selections", "Total Number", and "Price/M". Below the table, it lists "Other Selections" and "Requirements & Policies".

Selections	Total Number	Price/M
Total file	18,188,721	80.00

Minimum order: 10,000.

Other Selections
 Household income, presence of children, age, marital status, gender, 10.00/M extra; geography, education, 8.00/M extra; mail order buyer, 10.00/M extra; 1 month hotline, 12.00/M extra; 3 month hotline, 8.00/M extra; full lifestyle, demographic, buying behavior, interest.

Requirements & Policies

REQUIREMENTS & POLICIES

Commission / Credit Policy
 20% commission to brokers. 15% commission to agencies.

Update Schedule
 Updated monthly.

Method of Addressing
 FTP, e-mail, 50.00 fee.

Restrictions
 Net name is allowed.

19 See Exhibit D hereto.

20 **B. Apple Discloses its Customers' Personal Listening Information to**
 21 **Various Third-Party Mobile Application Developers, Who in Turn**
 22 **Rediscover Such Information to Other Third Parties**

23 51. Additionally, Apple has disclosed and continues to disclose its customers'
 24 Personal Listening Information to developers of iOS mobile applications, who in turn
 have disclosed and continue to disclose such data to other third parties for profit.

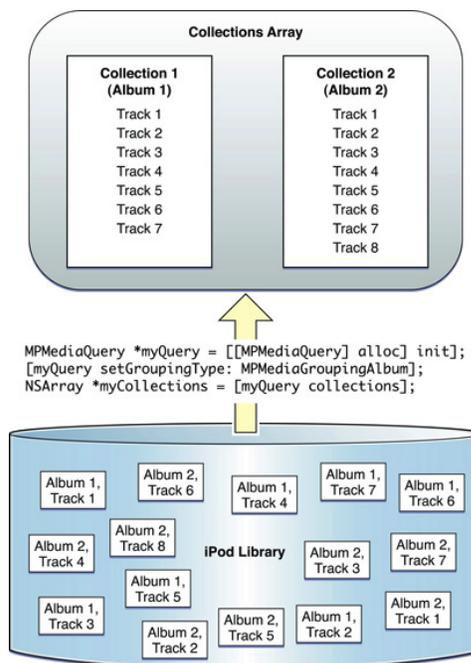
1 52. During the relevant time period, Apple has intentionally transmitted,
2 either directly or through an intermediary or intermediaries, its customers' Personal
3 Listening Information to the developers of mobile applications programmed with
4 Apple's iOS SDK, without first obtaining the requisite consent of its customers.

5 53. Specifically, many mobile applications developed using Apple's iOS
6 SDK have been programmed to provide their developers with complete and total
7 access, via Apple's "MediaPlayer Framework API," to highly-detailed metadata
8 reflecting the full content of the iTunes music libraries of users of devices on which
9 such applications are installed (applications which, on information and belief, include
10 but are not limited to those developed by Pandora).

11 54. Thus, Apple's MediaPlayer Framework API, used in conjunction with the
12 iOS SDK, has enabled application developers to collect, via transmissions made by
13 Apple, metadata reflecting the specific titles of the music purchased by particular users
14 of the iOS-equipped devices on which applications utilizing this functionality are
15 installed. During the relevant time period, developers have accomplished this with as
16 little as a single line of code written into their mobile applications. For example, using
17 the `MPMediaQuery.songsQuery()` function of the MediaPlayer Framework API,
18 developers are able to grant themselves access to metadata that identifies the titles of
19 all of the songs that a particular user of their application has purchased on iTunes.²⁰

20
21 ²⁰ See Dodson, Ben, *Your Music Library is a Security and Privacy Risk on iOS*,
22 Jan. 13, 2016, available at <https://bendodson.com/weblog/2016/02/23/details-on-ios-9-3-media-library-additions/> (last accessed May 13, 2019) (a copy of which is attached
23 hereto as **Exhibit E**); Open Radar: Community Bug Reports, *No permission required*
24 *to access full music library metadata*, Jan. 13, 2016, available at <https://openradar.appspot.com/radar?id=6078139771912192> (last accessed May 9, 2019) (a copy of which is attached hereto as **Exhibit F**).

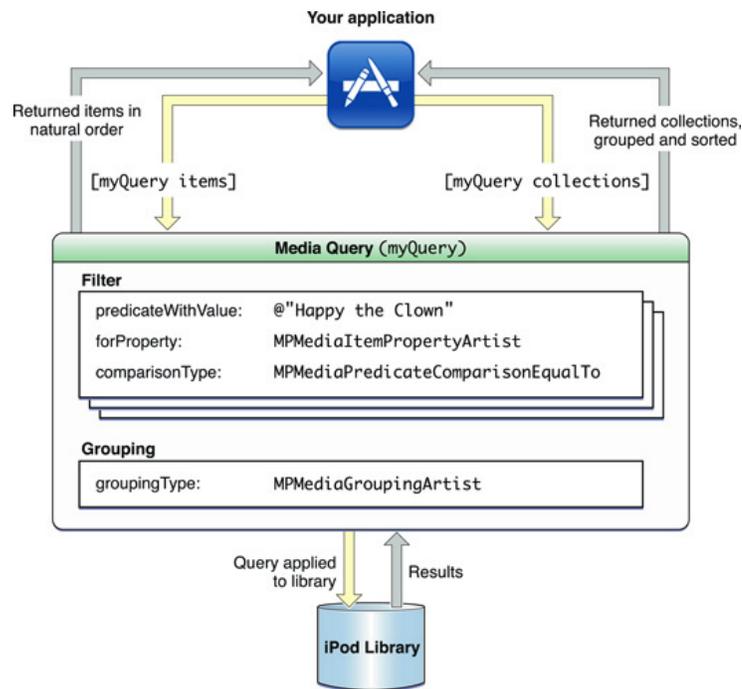
1 55. Further, during the relevant time period the MediaPlayer Framework API
 2 has enabled developers to “create arbitrarily complex queries” with “database access
 3 classes from from [the] API,” in order to collect users’ metadata filtered by specific
 4 categories of purchased music. For example, Apple’s MediaPlayer Framework API
 5 permits developers to retrieve the titles of specific “collections” (i.e., album names) of
 6 music that users of their applications have purchased, as well as the “tracks” (i.e.,
 7 songs) comprising such albums, as illustrated in the graphic below:



17 See Apple Inc., *iPod Library Access Programming Guide*, available at
 18 [https://developer.apple.com/library/archive/documentation/Audio/Conceptual/iPodLi](https://developer.apple.com/library/archive/documentation/Audio/Conceptual/iPodLibraryAccess_Guide/AboutiPodLibraryAccess/AboutiPodLibraryAccess.html#//apple_ref/doc/uid/TP40008765-CH103-SW16)
 19 [braryAccess_Guide/AboutiPodLibraryAccess/AboutiPodLibraryAccess.html#//apple](https://developer.apple.com/library/archive/documentation/Audio/Conceptual/iPodLibraryAccess_Guide/AboutiPodLibraryAccess/AboutiPodLibraryAccess.html#//apple_ref/doc/uid/TP40008765-CH103-SW16)
 20 [_ref/doc/uid/TP40008765-CH103-SW16](https://developer.apple.com/library/archive/documentation/Audio/Conceptual/iPodLibraryAccess_Guide/AboutiPodLibraryAccess/AboutiPodLibraryAccess.html#//apple_ref/doc/uid/TP40008765-CH103-SW16) (last accessed May 14, 2019) (section titled
 21 “About Collections and Playlists”), a copy of which is attached hereto as **Exhibit G**.

22 56. As another example, Apple’s MediaPlayer Framework API has enabled
 23 application developers to collect from their users’ iTunes music libraries metadata that
 24

1 identifies the titles of particular artists' albums that the applications' users have
 2 purchased from Apple, as illustrated in the graphic below:



12 See Ex. G (section titled "Getting Media Items Programmatically").

13 57. The metadata disclosed by Apple to these mobile application developers,
 14 by way of its proprietary MediaPlayer Framework API and/or similar such
 15 functionality, not only identifies the specific titles and/or the nature of the digitally-
 16 recorded music purchased by Apple's customers, but also is linked to data that
 17 identifies the individuals who purchased the music reflected in the metadata and/or the
 18 specific devices these individuals used to make such purchases, including in many
 19 cases the names and addresses of the purchasers of the music reflected in the metadata
 20 (including where a purchaser provided such personally-identifying information to the
 21 application developer as a prerequisite to installing the application or enrolling in
 22 services offered by the developer in its application, as is required of users of, for
 23 example, Pandora, Spotify, and innumerable other iOS mobile applications).

1 Accordingly, by engaging in these practices, Apple disclosed the Personal Listening
2 Information of its customers to various third-party mobile application developers.

3 58. On January 13, 2016, an iOS application developer named Ben Dodson
4 found the foregoing capabilities of Apple’s MediaPlayer Framework API so invasive
5 of privacy that he submitted a publicly-accessible “bug report” to Apple about it,
6 describing the issue as a “security” hole in which “[a]ll metadata can be pulled from
7 the [iTunes] library without the user knowing.” See Ex. F. Dodson’s bug report went
8 on to state as follows:

9 In recent years, iOS has made a concerted push to being
10 privacy focussed. However, one area this is not the case is
11 with the MediaPlayer framework and in particular the
12 MPMediaQuery.songsQuery() method. With that one line of
13 code, you can get the full metadata for every song in a user's
14 library without them ever knowing. This information could
15 be sent back to a server silently and then used for various
16 nefarious purposes such as:

14 - Building up a profile of that user in order to produce
targeted advertising

15 - Using the information as a reliable way of tracking someone
16 across multiple apps (as it can act as a unique identifier)

17 In my opinion, access to the music library should be
18 protected in much the same way as location, contacts,
19 calendars, or photos are with a requirement from the
developer to ask permission and for the user to be able to
grant permission and subsequently revoke it via the standard
iOS system preferences.

20 ...
21 I make use of this feature in my app Music Tracker
(<https://dodoapps.io/music-tracker>) but I'd feel much happier
22 about it if the user was allowing me access to their library
rather than it being automatic without their knowledge.

23 *Id.* Dobson noted that Apple’s MediaPlayer Framework API enabled developers of
24 mobile applications to use the “MPMediaQuery.songsQuery()” function of the API to

1 instruct Apple to transmit the “full music library metadata” from “any iOS device”
2 using “iOS 3.0 and above” on which the application had been installed. *See id.*

3 59. On January 22, 2016, Apple responded to Dobson’s “bug report,” stating
4 in pertinent part:

5 We are aware of this issue. It is being investigated. Thank
6 you for taking the time to pass it along to us. For the
7 protection of our customers, Apple does not publicly
8 disclose, discuss or confirm security issues until a full
9 investigation has occurred and any necessary patches or
10 releases are available.

11 *Id.*

12 60. Apple nonetheless failed to take any corrective measure to address the
13 issue until the public release of iOS 10.0, which occurred nearly eight months later on
14 or about September 13, 2016, and even then Apple merely began informing users that
15 their iTunes libraries may be “accessed” by developers of mobile applications utilizing
16 the MediaPlayer Framework API or similar functionality built with the iOS SDK.
17 Thus, the disclosures that Apple implemented in response to Dobson’s bug report (in
18 versions 10.0 and later of iOS) plainly fail to adequately put users on notice that their
19 Personal Listening Information will be extracted from their iTunes libraries and
20 disclosed by Apple to the developers of such applications. Accordingly, this disclosure
21 language has at all times material hereto been incapable of manifesting anyone’s
22 informed written consent to Apple’s practices of disclosing its customers’ Personal
23 Listening Information, even though the company was required to obtain such consent
24 prior to disclosing its customers’ Personal Listening Information pursuant to the
MIPPPA and the RIVRPA.

1 61. Still today, Apple permits application developers to use its APIs and other
2 developers' functionality in the same or substantially the same way as described above,
3 and thus still transfers to application developers the metadata containing its customers'
4 Personal Listening Information on demand.

5 62. For example, the current version of Apple's "Apple Music API," which is
6 part of Apple's "MusicKit" framework and is presently used by developers in
7 conjunction with the MediaPlayer Framework API, as discussed above, allows
8 developers to access information about the particular media – such as albums, songs,
9 artists, and playlists – that are located in a particular user's personal iCloud library.
10 Apple describes the Apple Music API as providing developers the following
11 functionality:

12 The Apple Music API is a web service that lets you access
13 information about the media found in the Apple Music
14 Catalog and the user's personal iCloud Music Library. Here's
15 what each one includes:

- 16 • The Apple Music Catalog includes all resources available
17 in Apple Music.
- 18 • The user's iCloud Music Library contains only those
19 resources that the user added to their personal library. For
20 example, it contains items from Apple Music, songs
21 purchased from iTunes Store, and imports from discs and
22 other apps. This library may include content not found in
23 the Apple Music Catalog.

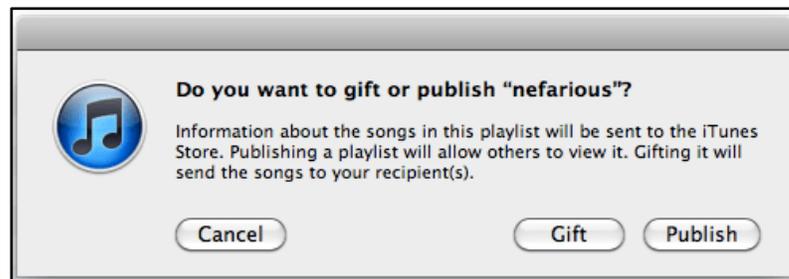
24 Use this service to retrieve information about albums, songs,
artists, playlists, music videos, Apple Music stations, ratings,
charts, recommendations, and the user's most recently played
content. With proper authorization from the user, you can
also create or modify playlists and apply ratings to the user's
content.

1 See Apple Inc., *Apple Music API*, available at
2 <https://developer.apple.com/documentation/applemusicapi> (last accessed May 24,
3 2019) (section titled “Overview”) (emphasis added), a copy of which is attached hereto
4 as **Exhibit H**. Notably, the Apple Music API only requires “proper authorization from
5 the user” in order for the developer to “create or modify playlists and apply ratings to
6 the user’s content.” Thus, developers using this API still have “read only” access to
7 metadata reflecting the contents of users’ iCloud Music Library (reflecting, inter alia,
8 the specific titles of the music and other items purchased from Apple via its iTunes
9 Store), via transmissions of such metadata by Apple to such developers on demand.

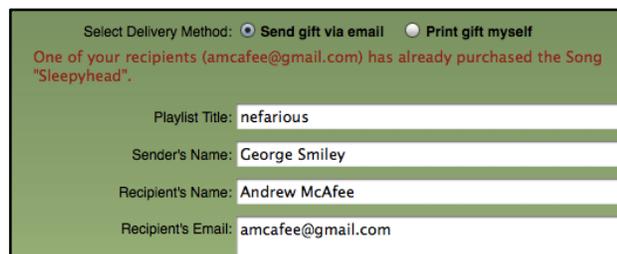
10 63. Developers are also able to access identifying information associated with
11 particular users, including via music user “tokens,” which are capable of association
12 with uniquely identifying information pertaining to individual users (including, for
13 example, by the numerous application developers who store the names and addresses
14 of their users collected during enrollment or otherwise). Requests to the Apple Music
15 API are sent using HTTPS commands and are associated with particular developers’
16 apps, by way of developer tokens that authenticate certain developers as “trusted
17 developers” and members of the Apple Developer Program. Thus, Plaintiffs are
18 informed and believe, and thereupon allege, that Apple readily possesses information
19 reflecting each of the instances in which it has disclosed its customers’ Personal
20 Listening Information, as well as data reflecting when and to whom such disclosures
21 were made.

22 64. Further, Apple has developed its own applications, web-based and
23 otherwise, to facilitate the transmission of its own customers’ Personal Listening
24

1 Information to other Apple customers. For example, during the relevant time period,
 2 Apple has transmitted or otherwise disclosed its customers' Personal Listening
 3 Information to other iTunes accountholders, including on information and belief
 4 entities engaged in the practices of collecting Personal Listening Information, in order
 5 to monetize Apple-developed platforms for its customers to "gift" songs from their
 6 iTunes playlists to other Apple customers, and to otherwise share content that its
 7 customers have purchased.²¹ Thus, during the relevant time period, when an iTunes
 8 user used Apple's functionality for "gifting" content to another user, including gifting
 9 a digitally-recorded song purchased on iTunes to another iTunes user, the gifter-user
 10 was presented a screen depicted, in pertinent part, as following:



15 To the extent a user to whom a particular song was being gifted had already purchased
 16 that song, Apple disclosed to the gifter that the giftee "has already purchased" that
 17 particular song, as shown in the following portion of a screenshot of such a disclosure:



22 ²¹ See A. McAfee, *SpyTunes*, available at
 23 <http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation/> (last
 24 accessed May 10, 2019) (attached hereto as **Exhibit I**); A. Howard, *Apple iTunes Gifts Users with a Privacy Hole*, Radar, available at <http://radar.oreilly.com/2011/02/itunes-privacy-hole.html> (last accessed May 11, 2019).

1 See Ex. G. By way of the foregoing tool, designed by Apple to further monetize content
2 that had already been purchased by its customers, as well as through other similar
3 publicly-accessible functionality provided by Apple, any person with an iTunes
4 account or any other entity (including those engaged in the business of collecting and
5 trafficking in Personal Listening Information) had the ability during at least a portion
6 of the relevant time period to obtain the Personal Listening Information of particular
7 Apple customers, via disclosures made to them by Apple. *See id.* (“This strikes me as
8 problematic. A person’s taste in media can be highly personal, yet all of Apple’s more
9 than 10 billion song and 200 million TV and movie downloads are potentially traceable
10 by . . . the world’s spies, stalkers, yellow journalists, and opposition researchers.”).

11 65. Plaintiffs are informed and believe, and thereupon allege, that Apple has
12 also sold, rented, transmitted, or otherwise disclosed its customers Personal Listening
13 Information to third party data analytics companies, including without limitation
14 Gracenote, Inc., The Nielsen Company, and MusicMetric.

15 66. As a result of Apple’s data compiling and sharing practices, companies
16 have obtained and continue to obtain the Personal Listening Information of Apple’s
17 customers, including those in Michigan and Rhode Island, together with additional
18 sensitive personal information that has been appended thereto by data appenders and
19 others (such as, for example, the income, gender, marital status, education, and family
20 composition (including the presence of children) of Apple’s customers).

21 67. Plaintiffs are informed and believe, and thereupon allege, that numerous
22 mobile application developers and other third parties to whom Apple has transmitted
23 and/or otherwise disclosed its customers’ Personal Listening Information (including
24

1 via its MediaPlayer, Apple Music and MusicKit APIs), either directly or indirectly
2 through an intermediary or intermediaries, have in turn sold, rented, transmitted, and
3 otherwise disclosed that Personal Listening Information (together with other sensitive
4 personal demographic and lifestyle information appended thereto by data appenders
5 and other entities) to other third parties, including other data brokers, data miners, data
6 appenders, and marketing companies.

7 68. Apple’s disclosures of Personal Listening Information have put its
8 customers, especially the more vulnerable members of society, at risk of serious harm
9 from scammers. For example, as a result of Apple’s disclosures of Personal Listening
10 Information, any person or entity could rent a list with the names and addresses of all
11 unmarried, college-educated women over the age of 70 with a household income of
12 over \$80,000 who have purchased country music from Apple using the iTunes Store
13 application that came pre-installed on their iPhones. Such a list is available for sale for
14 approximately \$136 per thousand customers listed.

15 69. Apple does not seek its customers’ prior written consent to the disclosure
16 of their Personal Listening Information and its customers remain unaware that their
17 Personal Listening Information and other sensitive data is being sold, rented and
18 exchanged on the open market.

19 70. By disclosing the nature and titles of its customers’ music purchases,
20 music-listening preferences, and personally-identifying information – which can
21 collectively “reveal intimate facts about our lives”²² – Apple has intentionally disclosed
22

23 ²² California’s Reader Privacy Act Signed into Law, EFF (Oct. 3, 2011),
24 <https://www.eff.org/press/archives/2011/10/03> (last visited May 14, 2019).

1 to third parties its customers' Personal Listening Information, without their consent, in
2 direct violation of Michigan's MIPPPA and Rhode Island's RIVRPA.

3 **PLAINTIFFS' EXPERIENCES**

4 **I. Plaintiff Leigh Wheaton**

5 71. Plaintiff Wheaton has on numerous occasions over the past three years,
6 while residing in Rhode Island, used an iPhone to purchase digital music, including
7 rock music, directly from Apple via its iTunes Store.

8 72. Prior to and at the time she purchased digital music, including rock music,
9 from Apple via its iTunes Store, Apple did not notify Plaintiff Wheaton that it would
10 disclose the Personal Listening Information of its customers to third parties, including,
11 but not limited to, developers of various mobile applications available for download in
12 its App Store, data aggregators, data appenders, data cooperatives, analytics
13 companies, and list brokers, and Plaintiff Wheaton has never authorized Apple to do
14 so. Furthermore, Plaintiff Wheaton was never provided any written notice that Apple
15 licenses, rents, exchanges, or otherwise discloses its customers' Personal Listening
16 Information to third parties, including, but not limited to, developers of various mobile
17 applications available for download in its App Store, data aggregators, data appenders,
18 data cooperatives, analytics companies, and list brokers, or any means of opting out of
19 such disclosures of her Personal Listening Information.

20 73. Apple nonetheless sold, rented, transmitted and/or otherwise disclosed
21 Plaintiff Wheaton's Personal Listening Information, either directly or through an
22 intermediary or intermediaries, to numerous third parties, including data miners,
23
24

1 appenders, aggregators, and analytics companies; mobile application developers; and
2 other third parties during the relevant time period.

3 74. Plaintiff Wheaton is informed and believes, and thereupon alleges, that
4 multiple mobile application developers and/or other third parties to whom Apple has
5 transmitted and/or otherwise disclosed her Personal Listening Information have in turn
6 sold, rented, transmitted, and otherwise disclosed her Personal Listening Information
7 (together with other sensitive personal demographic and lifestyle information appended
8 thereto by data appenders and other entities) to other third parties, including other data
9 brokers, data miners, data appenders, and marketing companies.

10 75. Because Apple sold, rented, transmitted and/or otherwise disclosed
11 Plaintiff Wheaton's Personal Listening Information, Plaintiff Wheaton now receives
12 junk mail from various companies and other organizations that do not offer products
13 or services through the mail. These unwarranted mailings waste Plaintiff Wheaton's
14 time, money, and resources. These unwarranted and harassing junk mailings, which are
15 attributable to Apple's unauthorized sale, rental, and/or other disclosure of her Personal
16 Listening Information, have wasted Plaintiff Wheaton's time, money, and resources.

17 76. Because Plaintiff Wheaton is entitled by law to privacy in her Personal
18 Listening Information, and paid money for the music she purchased and downloaded
19 from Apple via its iTunes Store, Apple's disclosure of her Personal Listening
20 Information deprived Plaintiff Wheaton of the full set of benefits to which she was
21 entitled as a part of her digital music purchases, thereby causing her economic harm.
22 Accordingly, what Plaintiff Wheaton received (digital music purchases without
23 statutory privacy protections) was less valuable than what she paid for (digital music
24

1 purchases with statutory privacy protections), and she would not have been willing to
2 pay as much, if at all, for the music she purchased from Apple via its iTunes Store had
3 she known that Apple would disclose her Personal Listening Information.

4 **II. Plaintiff Jill Paul**

5 77. Plaintiff Jill Paul has on numerous occasions over the past three years,
6 while residing in Michigan, used an iPhone to purchase digital music, including rock
7 music, directly from Apple via its iTunes Store.

8 78. Prior to and at the time she purchased digital music, including rock music,
9 from Apple via its iTunes Store, Apple did not notify Plaintiff Jill Paul that it would
10 disclose the Personal Listening Information of its customers to third parties, including,
11 but not limited to, developers of various mobile applications available for download in
12 its App Store, data aggregators, data appenders, data cooperatives, analytics
13 companies, and list brokers, and Plaintiff Jill Paul has never authorized Apple to do so.
14 Furthermore, Plaintiff Jill Paul was never provided any written notice that Apple
15 licenses, rents, exchanges, or otherwise discloses its customers' Personal Listening
16 Information to third parties, including, but not limited to, developers of various mobile
17 applications available for download in its App Store, data aggregators, data appenders,
18 data cooperatives, analytics companies, and list brokers, or any means of opting out of
19 such disclosures of her Personal Listening Information.

20 79. Apple nonetheless sold, rented, transmitted and/or otherwise disclosed
21 Plaintiff Jill Paul's Personal Listening Information, either directly or through an
22 intermediary or intermediaries, to numerous third parties, including data miners,
23
24

1 appenders, aggregators, and analytics companies; mobile application developers; and
2 other third parties during the relevant time period.

3 80. Plaintiff Jill Paul is informed and believes, and thereupon alleges, that
4 multiple mobile application developers and/or other third parties to whom Apple has
5 transmitted and/or otherwise disclosed her Personal Listening Information have in turn
6 sold, rented, transmitted, and otherwise disclosed her Personal Listening Information
7 (together with other sensitive personal demographic and lifestyle information appended
8 thereto by data appenders and other entities) to other third parties, including other data
9 brokers, data miners, data appenders, and marketing companies.

10 81. Because Apple sold, rented, transmitted and/or otherwise disclosed
11 Plaintiff Jill Paul's Personal Listening Information, Plaintiff Jill Paul now receives junk
12 mail from various companies and other organizations that do not offer products or
13 services through the mail. These unwarranted and harassing junk mailings, which are
14 attributable to Apple's unauthorized sale, rental, and/or other disclosure of her Personal
15 Listening Information, have wasted Plaintiff Jill Paul's time, money, and resources.

16 82. Because Plaintiff Jill Paul is entitled by law to privacy in her Personal
17 Listening Information, and paid money for the music she purchased and downloaded
18 from Apple via its iTunes Store, Apple's disclosure of her Personal Listening
19 Information deprived Plaintiff Jill Paul of the full set of benefits to which she was
20 entitled as a part of her digital music purchases, thereby causing her economic harm.
21 Accordingly, what Plaintiff Jill Paul received (digital music purchases without
22 statutory privacy protections) was less valuable than what she paid for (digital music
23 purchases with statutory privacy protections), and she would not have been willing to
24

1 pay as much, if at all, for the music she purchased from Apple via its iTunes Store had
2 she known that Apple would disclose her Personal Listening Information.

3 **III. Plaintiff Trevor Paul**

4 83. Plaintiff Trevor Paul has on numerous occasions over the past three years,
5 while residing in Michigan, used an iPhone to purchase digital music, including rock
6 music, directly from Apple via its iTunes Store.

7 84. Prior to and at the time he purchased digital music, including rock music,
8 from Apple via its iTunes Store, Apple did not notify Plaintiff Trevor Paul that it would
9 disclose the Personal Listening Information of its customers to third parties, including,
10 but not limited to, developers of various mobile applications available for download in
11 its App Store, data aggregators, data appenders, data cooperatives, analytics
12 companies, and list brokers, and Plaintiff Trevor Paul has never authorized Apple to
13 do so. Furthermore, Plaintiff Trevor Paul was never provided any written notice that
14 Apple licenses, rents, exchanges, or otherwise discloses its customers' Personal
15 Listening Information to third parties, including, but not limited to, developers of
16 various mobile applications available for download in its App Store, data aggregators,
17 data appenders, data cooperatives, analytics companies, and list brokers, or any means
18 of opting out of such disclosures of his Personal Listening Information.

19 85. Apple nonetheless sold, rented, transmitted and/or otherwise disclosed
20 Plaintiff Trevor Paul's Personal Listening Information, either directly or through an
21 intermediary or intermediaries, to numerous third parties, including data miners,
22 appenders, aggregators, and analytics companies; mobile application developers; and
23 other third parties during the relevant time period.

24

1 86. Plaintiff Trevor Paul is informed and believes, and thereupon alleges, that
2 multiple mobile application developers and/or other third parties to whom Apple has
3 transmitted and/or otherwise disclosed his Personal Listening Information have in turn
4 sold, rented, transmitted, and otherwise disclosed his Personal Listening Information
5 (together with other sensitive personal demographic and lifestyle information appended
6 thereto by data appenders and other entities) to other third parties, including other data
7 brokers, data miners, data appenders, and marketing companies.

8 87. Because Apple sold, rented, transmitted and/or otherwise disclosed
9 Plaintiff Trevor Paul's Personal Listening Information, Plaintiff Trevor Paul now
10 receives junk mail from various companies and other organizations that do not offer
11 products or services through the mail. These unwarranted and harassing junk mailings,
12 which are attributable to Apple's unauthorized sale, rental, and/or other disclosure of
13 his Personal Listening Information, have wasted Plaintiff Trevor Paul's time, money,
14 and resources.

15 88. Because Plaintiff Trevor Paul is entitled by law to privacy in his Personal
16 Listening Information, and paid money for the music he purchased and downloaded
17 from Apple via its iTunes Store, Apple's disclosure of his Personal Listening
18 Information deprived Plaintiff Trevor Paul of the full set of benefits to which he was
19 entitled as a part of his digital music purchases, thereby causing him economic harm.
20 Accordingly, what Plaintiff Trevor Paul received (digital music purchases without
21 statutory privacy protections) was less valuable than what he paid for (digital music
22 purchases with statutory privacy protections), and he would not have been willing to
23
24

1 pay as much, if at all, for the music he purchased from Apple via its iTunes Store had
2 he known that Apple would disclose his Personal Listening Information.

3 **CLASS ACTION ALLEGATIONS**

4 89. Plaintiff Wheaton brings this action pursuant to Federal Rules of Civil
5 Procedure 23(a), (b)(2), and (b)(3) on behalf of herself and a class of similarly-situated
6 Rhode Island residents (the “RI Class”), defined as follows:

7 All residents of Rhode Island who, at any time during the
8 applicable statutory period, had their Personal Listening
9 Information disclosed to third parties by Apple without their
10 consent.

11 90. Plaintiffs Jill Paul and Trevor Paul bring this action pursuant to Federal
12 Rules of Civil Procedure 23(a), (b)(2), and (b)(3) on behalf of themselves and a class
13 of similarly-situated Michigan residents (the “MI Class”), defined as follows:

14 All residents of Michigan who, at any time between May 24,
15 2016 and July 30, 2016, had their Personal Listening
16 Information disclosed to third parties by Apple without their
17 consent.

18 91. The RI Class and the MI Class are referred to herein collectively at times
19 as the “Classes”.

20 92. Excluded from the Classes is any entity in which Apple has a controlling
21 interest, and officers or directors of Apple.

22 93. Members of the Classes are so numerous that their individual joinder
23 herein is impracticable, as they number, on information and belief, in the tens of
24 thousands for the RI Class and the hundreds of thousands for the MI Class. The precise
number of members of the Classes and their identities are unknown to Plaintiffs at this
time but may be determined through discovery. Members of the Classes may be

1 notified of the pendency of this action by mail and/or publication through the
2 distribution records of Apple.

3 94. Common questions of law and fact exist as to all members of the Classes
4 and predominate over questions affecting only individual members of the Classes.
5 Common legal and factual questions include, but are not limited to:

6 (a) For the RI Class: (1) whether Apple is a “retailer or distributor” of music
7 products; (2) whether Apple disclosed the “nature” of the music purchased by Plaintiff
8 Wheaton and the RI Class; (3) whether Apple obtained the requisite consent before
9 disclosing to third parties Plaintiff Wheaton’s and the RI Class’s Personal Listening
10 Information; (4) whether Apple’s disclosure of Plaintiff Wheaton’ and the RI Class’s
11 Personal Listening Information violated Rhode Island General Laws § 11-18-32; and
12 (5) whether Apple’s sale, rental, transmission, and/or disclosure of Plaintiff Wheaton’s
13 and the RI Class’s Personal Listening Information constitutes unjust enrichment.

14 (b) For the MI Class: (1) whether Apple is “engaged in the business of selling
15 at retail” digitally-recorded and downloadable “sound recordings”; (2) whether Apple
16 obtained the requisite consent before disclosing to third parties Plaintiffs’ and the MI
17 Class’s Personal Listening Information; (3) whether Apple’s disclosure of Plaintiffs’
18 and the MI Class’s Personal Listening Information violated the MIPPPA § 2; and (4)
19 whether Apple’s sale, rental, transmission, and/or disclosure of Plaintiffs’ and the MI
20 Class’s Personal Listening Information constitutes unjust enrichment.

21 95. The claims of the named Plaintiffs are typical of the claims of each of the
22 Classes in that the Classes and the named Plaintiffs sustained damages as a result of
23
24

1 Apple's uniform wrongful conduct, based upon Apple's disclosures of Plaintiffs' and
2 the Classes' Personal Listening Information.

3 96. Plaintiffs are adequate representatives of the Classes because their
4 interests do not conflict with the interests of the members of the Classes they seek to
5 represent, they have retained competent counsel experienced in prosecuting class
6 actions, and they intend to prosecute this action vigorously. The interests of the
7 members of the Classes will be fairly and adequately protected by Plaintiffs and their
8 counsel.

9 97. The class mechanism is superior to other available means for the fair and
10 efficient adjudication of the claims of the members of the Classes. Each individual
11 member of each of the Classes may lack the resources to undergo the burden and
12 expense of individual prosecution of the complex and extensive litigation necessary to
13 establish Apple's liability. Individualized litigation increases the delay and expense to
14 all parties and multiplies the burden on the judicial system presented by the complex
15 legal and factual issues of this case. Individualized litigation also presents a potential
16 for inconsistent or contradictory judgments. In contrast, the class action device presents
17 far fewer management difficulties and provides the benefits of single adjudication,
18 economy of scale, and comprehensive supervision by a single court on the issue of
19 Apple's liability. Class treatment of the liability issues will ensure that all claims and
20 claimants are before this Court for consistent adjudication of the liability issues.

21
22
23
24

1 **CLAIMS FOR RELIEF**

2 **FIRST CLAIM FOR RELIEF**
3 **VIOLATION OF THE RIVRPA (R.I. Gen. Laws § 11-18-32)**
4 **(By Plaintiff Wheaton on Behalf of Herself and the RI Class Against Apple)**

5 98. Plaintiff Wheaton repeats the allegations contained in the foregoing
6 paragraphs as if fully set forth herein.

7 99. Plaintiff Wheaton brings this claim on behalf of herself and the members
8 of the RI Class against Defendant Apple.

9 100. Through its iTunes Store mobile application, Apple sells and rents
10 digitally-recorded music products to consumers at retail and distributes those products
11 to consumers. *See* R.I. Gen. Laws § 11-18-32(a).

12 101. The digitally-recorded music that Plaintiff Wheaton purchased from
13 Apple via its iTunes Store are published materials that are “like” “records” and/or
14 “cassettes” within the meaning of R.I. Gen. Laws § 11-18-32(a).

15 102. By purchasing digitally-recorded music from Apple via its iTunes Store
16 platform, Plaintiff Wheaton purchased materials that are “like” “records” and/or
17 “cassettes,” from a “retailer or distributor of those products” within the meaning of R.I.
18 Gen. Laws § 11-18-32(a). *See* R.I. Gen. Laws § 11-18-32(a).

19 103. At all times relevant, and beginning on the dates that Plaintiff Wheaton
20 first purchased music from Apple via the iTunes Store, Apple disclosed to third persons
21 Plaintiff Wheaton’s Personal Listening Information — which identified her address
22 and identified her as a purchaser of music of the rock genre, as well as a purchaser of
23 particular titles of music — in at least two ways.
24

1 104. First, Apple disclosed mailing lists containing Plaintiff Wheaton’s
2 Personal Listening Information, including the genres of music she has purchased, to
3 data aggregators, data appenders, marketing companies, mobile application developers,
4 and other third parties, who then supplemented the mailing lists with additional
5 sensitive information from their own databases and re-disclosed the lists to other third
6 parties for profit.

7 105. Second, Apple disclosed the Personal Listening Information of Plaintiff
8 Wheaton, including the genres and titles of music she has purchased, to numerous iOS
9 mobile application developers and other third parties, who have in turn disclosed such
10 data to other third parties for profit.

11 106. Additionally, Plaintiff Wheaton is informed and believes, and thereupon
12 alleges, that Apple has also sold, rented, transmitted, or otherwise disclosed her
13 Personal Listening Information and that of the other members of the RI Class to third
14 party data analytics companies, without their consent, including without limitation to
15 Gracenote, Inc., The Nielsen Company, and MusicMetric.

16 107. At all times relevant, and beginning on the dates that Plaintiff Wheaton
17 first purchased music from Apple via the iTunes Store, various third parties have, upon
18 receiving the Personal Listening Information of Plaintiff Wheaton and the other
19 members of the RI Class from Apple, further re-disclosed Plaintiff Wheaton’s and the
20 RI Class’s Personal Listening Information to other third persons, including data
21 aggregators, data appenders, marketing companies, mobile application developers, and
22 other third parties.

23
24

1 108. Because the mailing lists disclosed by Apple and redisclosed by other
2 downstream entities included additional information from the data aggregators and
3 appenders, the lists were more valuable, and Apple and the other third-party traffickers
4 of such data were able to increase their profits gained from the mailing list rentals
5 and/or exchanges.

6 109. By selling, renting, transmitting, and/or otherwise disclosing its customer
7 lists, together with its customers' addresses and the genres and/or titles of the music
8 they purchased, Apple disclosed to persons other than Plaintiff Wheaton records which
9 would identify her name, address, and the "nature" of the music she purchased from
10 Apple. *See* R.I. Gen. Laws § 11-18-32(a).

11 110. Plaintiff Wheaton and the members of the RI Class never consented to
12 Apple disclosing their Personal Listening Information to anyone.

13 111. Worse yet, Plaintiff Wheaton and the members of the RI Class did not
14 receive notice before Apple disclosed their Personal Listening Information to third
15 parties.

16 112. Apple's disclosures of Plaintiff Wheaton's and the RI Class's Personal
17 Listening Information were not made pursuant to lawful compulsion.

18 113. Apple's disclosures of Plaintiff Wheaton's and the RI Class's Personal
19 Listening Information were made to third parties, including, but not limited to, data
20 aggregators, data appenders, data cooperatives, direct-mail advertisers, marketers,
21 mobile application developers, and other third parties, in order to increase Apple's
22 revenue.

23
24

1 114. By disclosing Plaintiff Wheaton’s and the RI Class’s Personal Listening
2 Information, Apple violated Plaintiff’s and the RI Class’s statutorily-protected right to
3 privacy in their music-listening habits. *See* R.I. Gen. Laws § 11-18-32(a).

4 115. Additionally, because Plaintiff Wheaton and the members of the RI Class
5 paid Apple for the music they purchased from Apple’s iTunes Store platform, and
6 because Apple was obligated to comply with the RIVRPA, Apple’s unlawful disclosure
7 of Plaintiff Wheaton’s and the other RI Class members’ Personal Listening Information
8 deprived Plaintiff Wheaton and the RI Class members of the full value of their paid-
9 for digitally-recorded music. Because Plaintiff Wheaton and the other RI Class
10 members ascribe monetary value to the privacy of their Personal Listening Information,
11 Apple’s unlawful sales, rentals, transmissions, and/or other disclosures of their
12 Personal Listening Information caused them to receive less value than they paid for,
13 thereby causing them economic harm.

14 116. Likewise, because Plaintiff Wheaton and the other RI Class members
15 ascribe monetary value to the privacy of their Personal Listening Information, a
16 purchase of digitally-recorded that includes privacy protections for their Personal
17 Listening Information is more valuable than one that does not.

18 117. Accordingly, had Plaintiff Wheaton been adequately informed of Apple’s
19 disclosure practices, she would not have been willing to purchase the digitally-recorded
20 music that she bought from Apple via its iTunes Store at the prices charged, if at all.
21 Thus, Apple’s unlawful disclosures caused Plaintiff Wheaton economic harm.

22
23
24

1 118. Apple’s disclosures of Plaintiff Wheaton’s Personal Listening
2 Information to third parties has also caused an influx of third party print advertisements
3 and e-mail spam to Plaintiff Wheaton’s postal mailbox and e-mail inbox.

4 119. As a result of Apple’s unlawful disclosures of their Personal Listening
5 Information, Plaintiff Wheaton and the members of the RI Class have suffered privacy
6 and economic injuries. On behalf of herself and the RI Class, Plaintiff Wheaton seeks:
7 (1) an injunction requiring Apple to obtain consent from Rhode Island customers prior
8 to disclosing their Personal Listening Information as required by the RIVRPA; (2)
9 \$250.00 for each RI Class member for each violation committed by Apple pursuant to
10 R.I. Gen. Laws § 11-18-32(d); and (3) costs and reasonable attorneys’ fees pursuant to
11 R.I. Gen. Laws § 11-18-32(d).

12 **SECOND CLAIM FOR RELIEF**
13 **VIOLATION OF THE MIPPPA**

14 **(H.B. 5331, 84th Leg., Reg. Sess., P.A. No. 378, §§ 1-4 (Mich. 1988)**
15 **(By the MI Plaintiffs on Behalf of Themselves and the MI Class Against Apple)**

16 120. Plaintiffs Jill Paul and Trevor Paul (hereinafter the “MI Plaintiffs”) repeat
17 the allegations contained in the foregoing paragraphs as if fully set forth herein.

18 121. The MI Plaintiffs bring this claim on behalf of themselves and the
19 members of the MI Class against Apple.

20 122. The digitally-recorded music that Apple sells via its iTunes Store
21 application constitute “sound recordings” within the meaning of MIPPPA § 2.

22 123. Through its iTunes Store mobile application, Apple is engaged in the
23 business of selling and renting digitally-recorded music products to consumers at retail.
24

1 124. By purchasing and/or renting digitally-recorded rock music via the iTunes
2 Store platform, each of the MI Plaintiffs purchased “sound recordings” directly from
3 Apple. *See id.*

4 125. Because the MI Plaintiffs purchased sound recordings directly from
5 Apple, the MI Plaintiffs are “customers” within the meaning of the MIPPPA. *See*
6 MIPPPA § 1(a).

7 126. At various times between May 24, 2016 and July 30, 2016, Apple
8 disclosed to third persons the MI Plaintiffs’ Personal Listening Information, which
9 identified them as purchasers of particular genres of music and of particular titles of
10 music, in at least two ways.

11 127. First, between May 24, 2016 and July 30, 2016, Apple disclosed mailing
12 lists containing the MI Plaintiffs’ Personal Listening Information, including the genres
13 of music they have purchased, to data aggregators, data appenders, marketing
14 companies, mobile application developers, and other third parties, who then
15 supplemented the mailing lists with additional sensitive information from their own
16 databases and re-disclosed the lists to other third parties for profit.

17 128. Second, between May 24, 2016 and July 30, 2016, Apple disclosed the
18 Personal Listening Information of the MI Plaintiffs, including the genres and titles of
19 music they have purchased, to numerous third-party iOS mobile application developers
20 and other third parties, who have in turn disclosed such data to other third parties for
21 profit.

22 129. Additionally, the MI Plaintiffs are informed and believe, and thereupon
23 allege, that Apple has also sold, rented, transmitted, or otherwise disclosed their
24

1 Personal Listening Information and that of the other members of the MI Class to third
2 party data analytics companies, without their consent, including without limitation to
3 Gracenote, Inc., The Nielsen Company, and MusicMetric.

4 130. By selling, renting, transmitting, and/or otherwise disclosing its customer
5 lists together with the genres and/or titles of the music purchased by its customers
6 between May 24, 2016 and July 30, 2016, Apple disclosed to persons other than the
7 MI Plaintiffs records or information concerning the MI Plaintiffs' purchases of
8 digitally-recorded music, i.e., "sound recordings," from Apple. *See* R.I. Gen. Laws §
9 11-18-32(a).

10 131. The information Apple disclosed indicates the MI Plaintiffs' names and
11 addresses, as well as information indicating that they had purchased particular genres
12 and titles of music from Apple. Accordingly, the records or information disclosed by
13 Apple indicated the MI Plaintiffs' identities. *See* MIPPPA § 2.

14 132. The MI Plaintiffs and the members of the MI Class never consented to
15 Apple disclosing their Personal Listening Information to anyone.

16 133. The MI Plaintiffs and the members of the MI Class did not receive notice
17 before Apple disclosed their Personal Listening Information to third parties.

18 134. Apple's disclosures of the MI Plaintiffs' and the MI Class's Personal
19 Listening Information between May 24, 2016 and July 30, 2016 were not made
20 pursuant to a court order, search warrant, or grand jury subpoena.

21 135. Apple's disclosures of the MI Plaintiffs' and the MI Class's Personal
22 Listening Information between May 24, 2016 and July 30, 2016 were not made to
23 collect payment for their music purchases.

24

1 136. Apple’s disclosures of the MI Plaintiffs’ Personal Listening Information
2 between May 24, 2016 and July 30, 2016 were made to third parties, including, but not
3 limited to, data aggregators, data appenders, data cooperatives, direct-mail advertisers,
4 marketers, mobile application developers, and other third parties, in order to increase
5 Apple’s revenue. Accordingly, Apple’s disclosures were not made for the exclusive
6 purpose of marketing goods and services directly to the MI Plaintiffs and the members
7 of the MI Class.

8 137. By disclosing the MI Plaintiffs’ Personal Listening Information between
9 May 24, 2016 and July 30, 2016, Apple violated Plaintiff’s and the Class’s statutorily-
10 protected right to privacy in their music-listening habits. *See* MIPPPA § 2.

11 138. Additionally, because the MI Plaintiffs and the members of the MI Class
12 paid Apple for the music they purchased from Apple’s iTunes Store platform, and
13 because Apple was obligated to comply with the MIPPPA, Apple’s unlawful disclosure
14 of the MI Plaintiffs’ and the other MI Class members’ Personal Listening Information
15 deprived Plaintiffs and the RI Class members of the full value of their paid-for digitally-
16 recorded music. Because the MI Plaintiffs and the other MI Class members ascribe
17 monetary value to the privacy of their Personal Listening Information, Apple’s
18 unlawful sales, rentals, transmissions, and/or other disclosures of their Personal
19 Listening Information caused them to receive less value than they paid for, thereby
20 causing them economic harm.

21 139. Likewise, because the MI Plaintiffs and the other MI Class members
22 ascribe monetary value to the privacy of their Personal Listening Information, a
23
24

1 purchase of digitally-recorded that includes privacy protections for their Personal
2 Listening Information is more valuable than one that does not.

3 140. Accordingly, had the MI Plaintiffs been adequately informed of Apple's
4 disclosure practices, they would not have been willing to purchase the digitally-
5 recorded music that they bought from Apple via its iTunes Store at the prices charged,
6 if at all. Thus, Apple's unlawful disclosures caused the MI Plaintiffs economic harm.

7 141. Apple's disclosure of the MI Plaintiffs' Personal Listening Information to
8 third parties between May 24, 2016 and July 30, 2016 has also caused an influx of third
9 party print advertisements and e-mail spam to the MI Plaintiffs' mailboxes and inboxes.

10 142. As a result of Apple's unlawful disclosures of their Personal Listening
11 Information, the MI Plaintiffs and the members of the MI Class have suffered privacy
12 and economic injuries. On behalf of themselves and the MI Class, the MI Plaintiffs
13 seek: (1) an injunction requiring Apple to obtain consent from Michigan customers
14 prior to disclosing their Personal Listening Information as required by the MIPPPA;
15 (2) \$5,000.00 for each MI Class member for each violation committed by Apple
16 pursuant to MIPPPA § 5(a); and (3) costs and reasonable attorneys' fees pursuant to
17 MIPPPA § 5(b).

18 **THIRD CLAIM FOR RELIEF**
19 **UNJUST ENRICHMENT**

20 **(Brought by all Plaintiffs on Behalf of Themselves**
21 **And Members of Both Classes Against Apple)**

22 143. Plaintiffs repeat the allegations contained in the paragraphs above as if
23 fully set forth herein.

24 144. Plaintiffs all bring this claim individually and on behalf of the members
of both Classes against Apple.

1 145. Plaintiffs and the members of the Classes conferred benefits on Apple by
2 providing Apple with their Personal Listening Information and paying Apple for the
3 digitally-recorded music they purchased from Apple via its iTunes Store platform.

4 146. Apple received and retained the information and money belonging to
5 Plaintiffs and the Classes when Plaintiffs and the members of the Classes purchased
6 digitally-recorded music from Apple via its iTunes Store platform.

7 147. Because Apple received and processed payments for music purchases
8 from Plaintiffs and the members of the Classes, together with their Personal Listening
9 Information, and because Apple has employees and/or agents handling customer
10 accounts and billing as well as customer data, Apple appreciates or has knowledge of
11 such benefits.

12 148. Under the MIPPPA and RIVRPA, Plaintiffs and the members of the
13 Classes were entitled to confidentiality in their Personal Listening Information as part
14 of their purchases.

15 149. Under principles of equity and good conscience, because Apple failed to
16 comply with the MIPPPA and RIVRPA, Apple should not be allowed to retain the full
17 amount of money Plaintiffs and the members of the Classes paid for their purchases or
18 the money it received by selling, renting, transmitting, and/or otherwise disclosing the
19 Personal Listening Information of Plaintiffs and the members of the Classes.

20 150. Plaintiffs and the members of the Classes have suffered actual damages as
21 a result of Apple's unlawful conduct in the form of the value Plaintiffs and the members
22 of the Classes paid for and ascribed to the confidentiality of their Personal Listening
23 Information. This amount is tangible and will be calculated at trial.

24

1 151. Additionally, Plaintiffs and the members of the Classes have suffered
2 actual damages inasmuch as Apple's failure to inform them that it would disclose their
3 Personal Listening Information caused them to purchase digitally-recorded music via
4 the iTunes Store when they otherwise would not have.

5 152. Further, a portion of the purchase price of each song or album of music
6 sold to Plaintiffs and the members of the Classes was intended to ensure the
7 confidentiality of their Personal Listening Information, as required by the MIPPPA and
8 the RIVRPA. Because Plaintiffs and the members of the Classes were denied services
9 that they paid for and were entitled to receive—i.e., confidentiality in their Personal
10 Listening Information—and because Plaintiffs and the members of the Classes would
11 have commanded a discount to voluntarily forego those benefits, they incurred actual
12 monetary damages.

13 153. To prevent inequity, Apple should return to Plaintiffs and the members of
14 the Classes: (1) the value they ascribe to maintaining the confidentiality of their
15 Personal Listening Information, and (2) all money derived from Apple's sales, rentals,
16 transmissions, and/or other disclosures of the Personal Listening Information of
17 Plaintiffs and the members of the Classes.

18 154. Accordingly, Plaintiffs and the members of the Classes seek an order
19 declaring that Apple's conduct constitutes unjust enrichment, and awarding Plaintiffs
20 and the members of the Classes restitution in an amount to be calculated at trial equal
21 to the amount of money obtained by Apple through its sales, rentals, transmissions,
22 and/or other disclosures of the Personal Listening Information of Plaintiffs and the
23 members of the Classes.

24

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seek a judgment against Apple, individually and on behalf of all others similarly situated, as follows:

A. For an order certifying the Classes under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiffs as representatives of the Classes and Plaintiffs’ attorneys as Class Counsel to represent the Classes.

B. For an order declaring that Apple’s conduct as described herein violates the Video, Audio, And Publication Rentals Privacy Act, R.I. Gen. Laws § 11-18-32;

C. For an order declaring that Apple’s conduct as described herein violates Michigan’s Preservation of Personal Privacy Act, H.B. 5331, 84th Leg., Reg. Sess., P.A. No. 378, §§ 1-4 (Mich. 1988), *id.* § 5, added by H.B. 4694, 85th Leg., Reg. Sess., P.A. No. 206, § 1 (Mich. 1989);

D. For an order finding in favor of Plaintiffs and the Classes on all counts asserted herein;

E. For Apple to pay \$250 to Plaintiff Wheaton and each unnamed RI Class member, as provided by the Video, Audio, And Publication Rentals Privacy Act, R.I. Gen. Laws § 11-18-32(d);

F. For Apple to pay \$5,000 to Plaintiffs Jill Paul and Trevor Paul and each MI Class member, as provided by the Preservation of Personal Privacy Act, H.B. 5331, 84th Leg., Reg. Sess., P.A. No. 378, §§ 1-4 (Mich. 1988), *id.* § 5, added by H.B. 4694, 85th Leg., Reg. Sess., P.A. No. 206, § 1 (Mich. 1989);

G. For prejudgment interest on all amounts awarded;

H. For an order of restitution and all other forms of equitable monetary relief;

- 1 I. For injunctive relief as pleaded or as the Court may deem proper; and
2 J. For an order awarding Plaintiffs and the Classes their reasonable
3 attorneys' fees and expenses and costs of suit.

4 **DEMAND FOR JURY TRIAL**

5 Plaintiffs, on behalf of themselves and the Classes, hereby demand a trial by jury
6 pursuant to Federal Rule of Civil Procedure 38(b) on all claims so triable.

7 Dated: May 24, 2019

Respectfully submitted,

8

By: /s/ Frank S. Hedin

9

Frank S. Hedin

10

FRANK S. HEDIN (SBN 291289)

fhedin@hedinhall.com

11

DAVID W. HALL (SBN 274921)

dhall@hedinhall.com

12

HEDIN HALL LLP

Four Embarcadero Center, Suite 1400

San Francisco, California 94104

13

Telephone: (415) 766-3534

Facsimile: (415) 402-0058

14

15

TINA WOLFSON (SBN 174806)

twolfson@ahdootwolfson.com

16

ROBERT AHDOOT (SBN 172098)

rahdoot@ahdootwolfson.com

17

AHDOOT & WOLFSON, PC

10728 Lindbrook Dr.

Los Angeles, California 90024

18

Telephone: (310) 474-9111

Facsimile: (310) 474-8585

19

20

L. TIMOTHY FISHER (SBN 191626)

ltfisher@bursor.com

21

BURSOR & FISHER, P.A.

1990 North California Blvd., Suite 940

Walnut Creek, California 94596

22

Telephone: (925) 300-4455

Facsimile: (925) 407-2700

23

24

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24

JOSEPH I. MARCHESE*
jmarchese@bursor.com
PHILIP L. FRAIETTA*
pfraietta@bursor.com
BURSOR & FISHER, P.A.
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163

** Pro Hac Vice Application Forthcoming*
Counsel for Plaintiffs and the Putative Classes

EXHIBIT A

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF
AN ACT
RELATING TO CRIMINAL OFFENSES --
UNLAWFUL DISSEMINATION OF RECORDS

1 This act prohibits the revealing of records relating to the
2 rental of video or audio tapes or publications and makes any
3 violation punishable by a fine not exceeding \$1,000. per viola-
4 tion. This act also provides a civil penalty.

5 This act would take effect upon passage.

ES541/SUB A/2

EXHIBIT B



Washington Square Building, Suite 1025
Lansing, Michigan 48909
Phone: 517/373-6466

PRIVACY: SALES, RENTALS OF VIDEOS, ETC.

**House Bill 5331 as enrolled
Second Analysis (1-20-89)**

**Sponsor: Rep. David Honigman
House Committee: Judiciary
Senate Committee: Judiciary**

THE APPARENT PROBLEM:

During the period when Congressional confirmation hearings were being held on the nomination of Robert Bork to the Supreme Court, a Washington weekly obtained and published a list of videotapes rented under Bork's wife's account. Many found this to be an unwarranted invasion of privacy, and the incident prompted the introduction in Congress of a bill to protect the privacy of those who rent or buy videotapes. Many in Michigan also believe that one's choice in videos, records, and books is nobody's business but one's own, and suggest the enactment of a statute to explicitly protect a consumer's privacy in buying and borrowing such items.

THE CONTENT OF THE BILL:

The bill would create a new public act to preserve personal privacy with respect to the purchase, rental, or borrowing of written materials, sound recordings, and video recordings. Except as otherwise provided by law, a retailer, lender, or renter of such items could not disclose information — such as selections made — on a particular customer to any person other than that customer. Such information could be disclosed with the customer's written permission, under a court order, to the extent reasonably necessary to collect past-due payment, for the exclusive purpose of marketing goods and services directly to the consumer, or under a search warrant. Violation of the bill would be a misdemeanor.

FISCAL IMPLICATIONS:

The House Fiscal Agency says that the bill would have no fiscal implications. (1-18-89)

ARGUMENTS:

For:

The bill would recognize that a person's choice in reading, music, and video entertainment is a private matter, and not a fit subject for consideration by gossipy publications, employers, clubs, or anyone else, for that matter. The bill would complement the Library Privacy Act, which exempts library records on a person from disclosure under the Freedom of Information Act and prohibits disclosure absent a court order or the individual's consent.

Response: The bill, while laudable in its aims, may be unnecessary for libraries, which already are subject to civil penalties for violating the Library Privacy Act.

Against:

The bill could offer more in the way of recourse for injured parties if it provided for civil damages as well as criminal misdemeanor penalties. Civil remedies not only offer a person recompense for harm done: they free a person from having to rely on a prosecutor's office to pursue a case.

H.B. 5331 (1-20-89)

EXHIBIT C

iTunes and Pandora music Purchasers are consumers using major internet providers for their music listening pleasure. iTunes and Pandora Music Purchasers enjoy playing their favorite radio stations from home, work, or mobile devices. Individual song, video and record purchases and/or commercial free listening allow for a highly custom playlist along with a much wider geographical reach than local radio stations for a higher quality transmitted sound. These purchasers get access to more stations and a wider variety of programming options all hand selected by the individual. iTunes and Pandora Music Purchasers are constantly looking for the most up to date cutting edge technology. They are highly responsive to new technology, cell phones and apps, computers, vacation packages, coupons, deal saving offers, trial run offers, entertainment, satellite TV and sports offers.

SEGMENTS	PRICE	ID NUMBER
18,188,721 TOTAL UNIVERSE / BASE RATE	\$80.00/M	NextMark 385690
1 Month Hotline	+ \$12.00/M	Manager
3 Month Hotline	+ \$8.00/M	UNIVERSE
		18,188,721
		LIST TYPE
DESCRIPTION		Consumer 
iTunes and Pandora music Purchasers are consumers using major internet providers for their music listening pleasure. iTunes and Pandora Music Purchasers enjoy playing their favorite radio stations from home, work, or mobile devices. Individual song, video and record purchases and/or commercial free listening allow for a highly custom playlist along with a much wider geographical reach than local radio stations for a higher quality transmitted sound. These purchasers get access to more stations and a wider variety of programming options all hand selected by the individual.		SOURCE
		LIST MAINTENANCE
		Counts through 04/01/2019
		Last update 04/01/2019
		Next update 05/01/2019
		SELECTS
		AGE 10.00/M
		Buying Behavior
		Demographic
		Education 8.00/M
		Full Lifestyle
		GENDER 10.00/M
		Geography 8.00/M
		House Hold Income 10.00/M
		Interest
		Mail Order Buyer 10.00/M
		MARITAL STATUS 10.00/M
		PRESENCE OF CHILDREN 10.00/M
		GEOGRAPHY
		USA

iTunes and Pandora Music Purchasers are constantly looking for the most up to date cutting edge technology. They are highly responsive to new technology, cell phones and apps, computers, vacation packages, coupons, deal saving offers, trial run offers, entertainment, satellite TV and sports offers.

EXHIBIT D

LIST SELECTS

Counts Thru: May 2018

Selections	Total Number	Price/M
Total file	18,188,721	80.00

Minimum order: 10,000.

Other Selections

Household income, presence of children, age, marital status, gender, 10.00/M extra; geography, education, 8.00/M extra; mail order buyer, 10.00/M extra; 1 month hotline, 12.00/M extra; 3 month hotline, 8.00/M extra; full lifestyle, demographic, buying behavior, interest.

▲ **Requirements & Policies**

REQUIREMENTS & POLICIES

Commission / Credit Policy

20% commission to brokers. 15% commission to agencies.

Update Schedule

Updated monthly.

Method of Addressing

FTP, e-mail, 50.00 fee.

Restrictions

Net name is allowed.

EXHIBIT E

Ben Dodson

Freelance iOS, Apple Watch, and Apple TV Developer

HOME BLOG ABOUT PORTFOLIO MY APPS PROJECTS CONTACT

Details on the iOS 9.3 Media Library additions

February 23, 2016

UPDATE: Thanks to my raising this privacy concern, Apple have resolved this issue as of iOS 10. I've left the old post below for posterity.

Due to my article on music library security on iOS, I've found myself in the position of being misquoted or misunderstood on sites such as AppleInsider (mainly in the comments) with regards to the new media library APIs in iOS 9.3. This article is intended to clear up some misunderstandings that people have about these new APIs.

In iOS 9.3, there are several additions to the music library. Indeed, it is the first item listed in the What's New in iOS 9.3 developer document:

New methods in the Media Player and StoreKit frameworks let you add an Apple Music track to the music library and play it. First, use the `SKCloudServiceController` API to determine the current capabilities, such as if the device allows playback of Apple Music catalog tracks and the addition of tracks to the library. Then, you can use the `MPMediaLibrary` method `addItemWithProductID:completionHandler:` to add a track to the library and the `MPMusicPlayerController` method `setQueueWithStoreIDs:` to play a track.

Firstly, the StoreKit framework has been updated to include an `SKCloudServiceController` which basically gives an app the opportunity to request access to a user's media library and to check if they have the ability to stream Apple Music tracks and / or add those tracks to their iCloud Music library.

Next, `MPMusicPlayerController` has been updated with a new method named `setQueueWithStoreIDs` which allows you to basically hand over an array of Apple Music identifiers and have those play instantly in the Music app without leaving your own app. Interestingly, this allows you to Rickroll someone in just a few lines of code:

```
func play() {
    let trackID = "255991760" // use 302053341 in USA, 255991760 in UK
    let controller = MPMusicPlayerController()
    controller.setQueueWithStoreIDs([trackID])
    controller.play()
}
```

This API, whilst interesting, has a few issues; the identifiers for music tracks are different for each country so a US track will not play on a UK Apple Music account¹. There is also no error handling so it'll just silently fail if you give it an incorrect identifier or one from the wrong store.

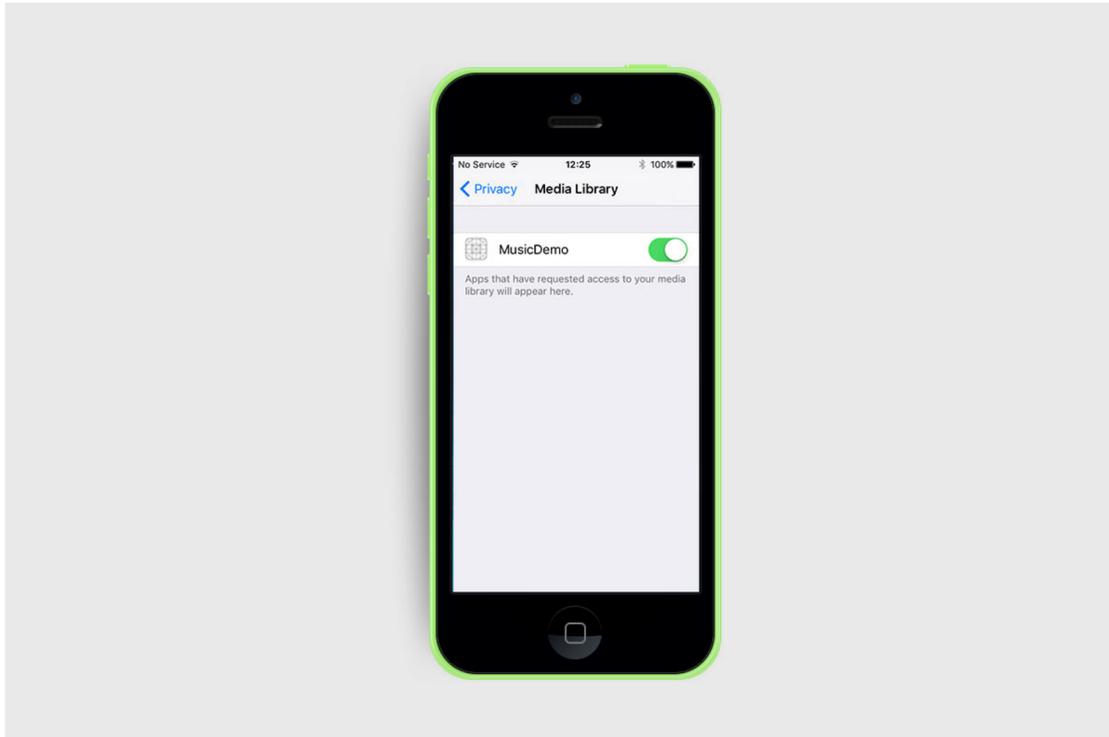
The final new addition is to `MPMediaLibrary` and is a method named `addItemWithProductID:completionHandler:.` This allows you to add an Apple Music track to the user's library as long as they gave permission via the `SKCloudServiceController` and they have a valid Apple Music account. I had some issues getting this working on an iPhone 5c but it worked just fine on an iPad Pro leading me to think this may be an API limited to 64-bit devices (although this is still in beta so that may change). However, the API does not allow you to add MP3s to your library or import Spotify tracks or anything like that; it is just a way to add Apple Music tracks to your library. Why is that useful? The scenario I envision is that it is for apps like Shazam that identify music and then traditionally give you a link to go and see it in Apple Music or the iTunes Store. With this new API, those apps can now add a button such as "add this track to your library?" which will allow them to automatically add the Apple Music track to the media library.

The new APIs do not do any of the following things:

- They do not allow apps to add music to your library if you are not using Apple Music
- They do not allow apps to add music to your library that is not available on Apple Music
- They do not allow apps to delete music from your library

- They do not allow apps to edit metadata on any music in your library (i.e. changing title, artist, genre, rating, artwork)

Crucially, and linking this back to my previous article, **this new permissions system is only for the new “add Apple Music tracks to your library API”**; apps do not require permission to scan through your library. I’m still hopeful this will be addressed as at present the ‘Privacy’ settings screen in iOS 9.3 is incredibly misleading:



I take serious issue with the phrase *“Apps that have requested access to your media library will appear here”* because it makes it sound like apps require permission to access your library which is just not true. My Music Tracker app continues to work unimpeded on iOS 9.3 with no need to request access and, as demonstrated above, you can start playing streamed music in the Music app without authorization. This is all true as of iOS 9.3 beta 4 so hopefully it may get resolved before the final version of iOS 9.3 is released next month.

(Update: This was not resolved in the public version of iOS 9.3)

If you have any queries about how these new APIs work or how they will or won't affect your media library, please feel free to contact me.

-
1. There is a new API to give you a storefront identifier (mine is "143444,29") but I'm not sure how you translate to a single language like "gb" for use with the iTunes Search API – if anyone can shed some light on that, please let me know!

Update, 10th Mar 2016: Thanks to [Loreto Parisi](#) for making me aware of the [iTunes Affiliate Link website](#) which contains a full list of the store identifiers and their respective ISO country codes which can be used with the iTunes Search API. I've [put together a simple class](#) to take care of this automatically.

Update, 31st Mar 2016: Thanks to [Matt Abras](#) it turns out that the above code isn't necessary; you can just use the undocumented `s=143444` instead of `country=gb` when using the [iTunes Search API](#). ! "

« The Divide #8 - Drunkstarter: A discussion
on crowdfunding

Storefront Additions: A simple way to convert
SKCloudServiceController store identifiers
into country codes »

I perform all freelance work through my company **Dodo Apps Ltd** (07856552) registered at The Bristol Office, 2nd Floor, 5 High Street, Westbury on Trym, Bristol, England, BS9 3BY

EXHIBIT F

Open Radar

Community bug reports

[Home](#) | [Recent Comments](#) | [Sign in](#)

No permission required to access full music library metadata

Originator: ben
Number: [rdar://24168798](#) Date Originated: 13th January 2016
Status: Duplicate/23416384 Resolved: Yes
Product: iOS SDK Product Version: 3.0+
Classification: Security Reproducible: Always

Summary:

In recent years, iOS has made a concerted push to being privacy focussed. However, one area this is not the case is with the MediaPlayer framework and in particular the `MPMediaQuery.songsQuery()` method. With that one line of code, you can get the full metadata for every song in a user's library without them ever knowing. This information could be sent back to a server silently and then used for various nefarious purposes such as:

- Building up a profile of that user in order to produce targeted advertising
- Using the information as a reliable way of tracking someone across multiple apps (as it can act as a unique identifier)

In my opinion, access to the music library should be protected in much the same way as location, contacts, calendars, or photos are with a requirement from the developer to ask permission and for the user to be able to grant permission and subsequently revoke it via the standard iOS system preferences.

Steps to Reproduce:

1. Import the "MediaPlayer" framework
2. Run the code `MPMediaQuery.songsQuery()` and loop through the results

Expected Results:

The user should be asked for permission for you to access their music library

Actual Results:

All metadata can be pulled from the library without the user knowing

Version:

iOS 3.0 and above

Notes:

I make use of this feature in my app Music Tracker (<https://dodoapps.io/music-tracker>) but I'd feel much happier about it if the user was allowing me access to their library rather than it being automatic without their knowledge.

Configuration:

Any iOS device

Comments

Follow up from Apple

Thank you for reporting this. We appreciate your assistance in helping us to maintain and improve the security of our products.

We are aware of this issue. It is being investigated. Thank you for taking the time to pass it along to us.

For the protection of our customers, Apple does not publicly disclose, discuss or confirm security issues until a full investigation has occurred and any necessary patches or releases are available.

We usually distribute information about security updates here: <http://support.apple.com/kb/HT201222>

By **ben** at Jan. 22, 2016, 10:13 a.m. (reply...)

Add a comment

Please note: Reports posted here will not necessarily be seen by Apple. All problems should be submitted at bugreport.apple.com before they are posted here. Please only post information for Radars that you have filed yourself, and please do not include Apple confidential information in your posts. Thank you!

Running on [Google App Engine](#) (HRD, Python 2.7). Source code on [GitHub](#). Answers to [Frequently Asked Questions](#). [On Twitter](#).

EXHIBIT G

Retired Document

Important: This document may not represent the best practices for current deployment. Links to downloads and other resources may no longer be valid. See MediaPlayer Framework API for the latest information.

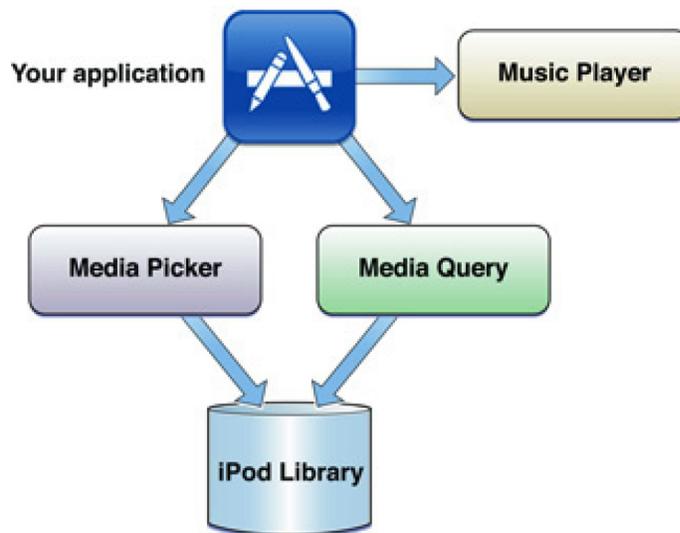
ce iPod library. The

iPod library is the set of media items on a device that a user has synced from iTunes on the desktop.

As shown in Figure 1–1, your application has two ways to retrieve items. The media picker, shown on the left, is an easy-to-use, pre-packaged view controller that behaves like the built-in iPod application’s music selection interface. For many applications, this is sufficient.

If the picker doesn’t provide the specialized access control that you want, the media query interface—shown to the lower right of your application in the figure—will. It supports predicate-based specification of items from the device iPod library.

Figure 1–1 Using iPod library access



As depicted to the right of your application in the figure, you then play the retrieved media items using the music player provided by this API.

As you can see, the classes in this API address two, usually distinct areas of development: database access—for finding media items to play—and music playback. However, you do not need to be a subject expert in either area to use this API effectively. iPod library access does the “heavy lifting” for you.

For example, the entirety of your music playback code is a single line—whether playing DRM-encrypted AAC files, Apple Lossless tracks ripped from a CD, audio podcasts encoded with iLBC, or audio books. The system automatically sets up buffering, chooses the appropriate codec, and sends the audio directly to the device output hardware.

Using a music player and the media item picker, you can implement music selection and playback without writing any code to access the iPod library. The database access classes provide a complete query system when you need it, and stay out of your way when you don’t.

Note: iPod library access applies only to audio-based media items. You cannot play video podcasts, movies, or television shows from the iPod library.

About Music Players

Your application uses a music player in a way that's similar to an end user operating the built-in iPod application. You can programmatically play, pause, seek, and so on.

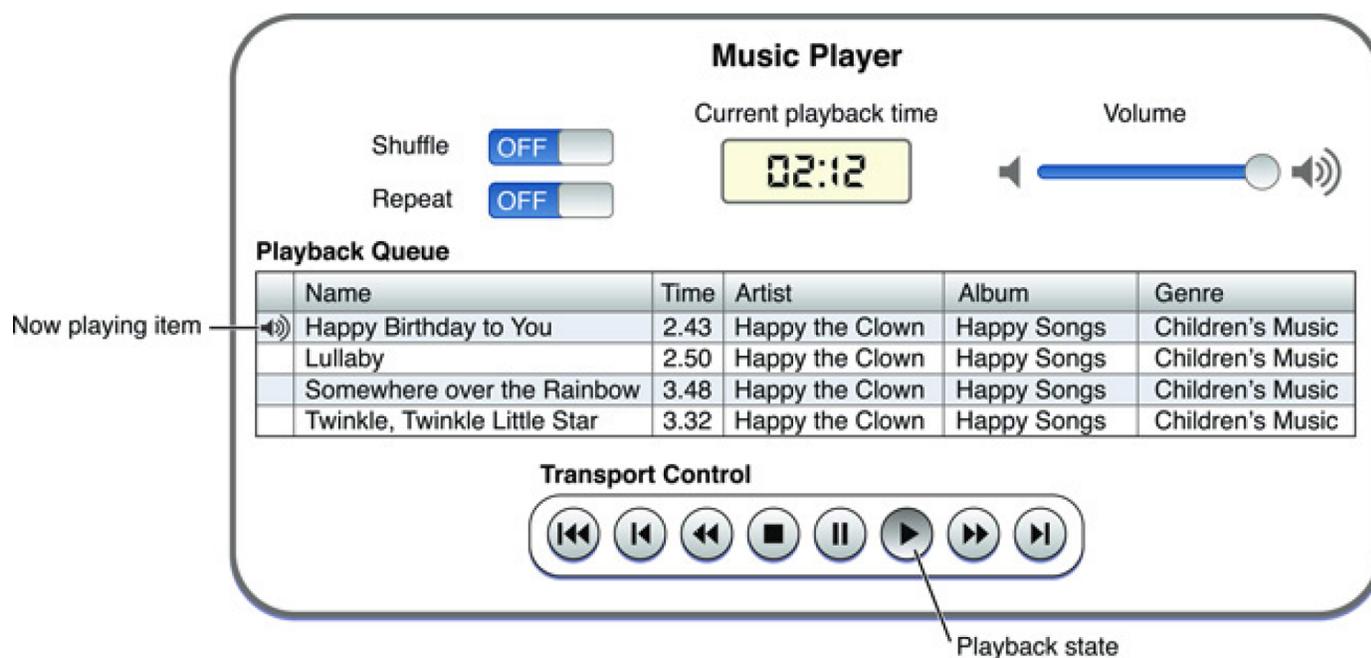
Music Player Basics and Terminology

A *music player* is the object you use for playing media items. It has a *playback queue*, which is a list of media items to play. A *media item* is a song, audio podcast, or audio book.

Media items get onto a device when a user syncs them from iTunes on the desktop. On the device, the complete set of media items is called the *iPod library*.

A music player knows which item is now playing or designated to play, and knows where in that item's timeline playback is at a given moment. These attributes are depicted schematically in Figure 1–2. (The figure is for explanation only. A music player does not provide a user interface.)

Figure 1–2 Schematic representation of a music player object



The *now playing* item has special status. For example, if a user pauses a song in the built-in iPod application, and then launches your application, your music player can continue playing that item from the same spot.

Additional properties round out the music player, making it highly flexible. As shown in the figure, a music player also has modes, playback state, and volume.

- *Shuffle mode* and *repeat mode* operate the same way they do in the built-in iPod app.

- *Playback state* is what you'd expect from any audio playback system: playing, stopped, paused, fast forward, or rewind. In addition, you can skip to the beginning of the next or previous media item and return to the start of a playback queue.
- *Volume* is full by default and can be set to any value down to silent.

You can obtain two flavors of music player, depending on the goals of your application.

- The *application music player* plays music locally within your application. It is not influenced by, nor does it affect, the state of the built-in iPod application. Specifically, your music player has a different now-playing item, playback state, and modes. When a user quits your application, music that you are playing stops.
- The *iPod music player*, in effect, employs the built-in iPod app on your behalf; it shares the iPod's state. When a user quits an app that is using this player, the music continues to play.

Finally, keep in mind the following two important points about using music players:

- Only one music player can play audio at a time.
- A music player can be used only on the main thread of your app.

Hello Music Player

Here is a bare bones *hello world*-style example that demonstrates library access and music playback. In a few minutes you can have a working, if minimal, music player. Lacking a user interface, this code queues up the entire device iPod library and starts playing immediately on launch.

Note: To follow these steps you'll need a provisioned device because the Simulator has no access to a device's iPod library.

1. Create a new Xcode project.

In Xcode, create a new project using the Window-based Application template. In the project window, add the `MediaPlayer` framework to the Frameworks group. Save the project.

2. Import the umbrella header file for the Media Player framework.

Add the following line to the `AppDelegate.h` file, after the existing `#import` line:

```
#import <MediaPlayer/MediaPlayer.h>
```

3. Add code to create a music player, assign it music to play, and start playback.

Open the project's `AppDelegate.m` implementation file. Before the end of the `applicationDidFinishLaunching:` block, add the three lines of code shown in Listing 1-1.

Listing 1-1 A very bare-bones music player

```
// instantiate a music player
MPMusicPlayerController *myPlayer =
```

```
[MPMusicPlayerController applicationMusicPlayer];

// assign a playback queue containing all media items on the device
[myPlayer setQueueWithQuery: [MPMediaQuery songsQuery]];

// start playing from the beginning of the queue
[myPlayer play];
```

Now, configure your project appropriately for your development device, which includes setting the code-signing identity and the bundle identifier. Also, ensure that the device has at least one song in its iPod library. Build and run the project. When the application launches on the device, the first song in the iPod library starts playing. The player continues to play through all the items in the iPod library or until you quit the application.

About Music Player Change Notifications

To keep track of what a music player is doing, you register for music player change notifications. This is essential for ensuring that your application's state and the music player's state are well coordinated.

For example, here is the sequence of events for correctly starting up music playback. Notice that, because music players operate on their own threads, you do not update your user interface until receiving the appropriate notification.

1. A user taps Play.
2. Your application invokes playback on the music player.
3. The music player starts playing and issues a playback-state-change notification.
4. Your application receives the notification and queries the music player's state, confirming that it is indeed playing.
5. Your application updates its user interface accordingly—perhaps changing the Play button to say Pause.

Music player change notifications support keeping track of playback state, the now-playing item, and the music player's playback volume. Using Media Playback explains how to use them.

Home Sharing and iPod Music Players

Starting in iOS 4, the built-in iPod and Videos apps can play media from shared libraries using Home Sharing. However, third-party apps using the Media Player framework still have access only to the device iPod library. This means that your app cannot display the title of a home-shared song in your user interface. Other playback information—such as current playback time and playback state—is available, however, when playing shared media.

About Media Items and the iPod Library

Media items—the songs, audio books, and audio podcasts in the iPod library—can have a wide range of metadata. You can use this metadata in building queries and in creating attractive displays of the media items in the user interface. Figure 1–3 gives you an idea of the character of a media item.

Figure 1–3 A media item and some of its metadata



All media item metadata is read-only. However, by using media item Persistent ID values, you can associate additional metadata that you manage in your application.

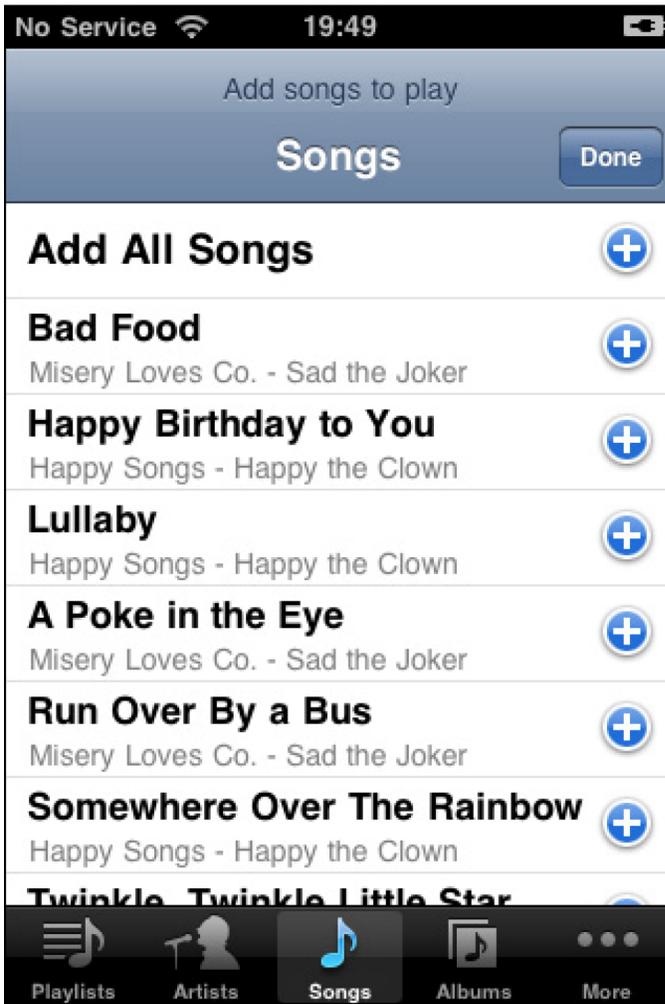
As Figure 1–3 suggests, an item's metadata can include more than one category of information. So-called *general properties* are those that can apply to any media item. These include "title," "artist," "artwork," and many others. The values of these properties typically do not change over time.

A media item can also have *user-defined properties* such as rating and last-played date. These properties update according to user activity, just as they do on the desktop.

The Media Item Picker

The simplest way to enable users to choose music is to use a *media item picker*—a fully-configured modal view controller. Its user interface is similar to the built-in iPod application's on-the-go interface, as shown in Figure 1–4.

Figure 1–4 The user interface of the media item picker



When the user taps Done, a delegate method that you implement receives the list of chosen media items and then dismisses the picker's view.

It's important to know that the similarity between the media item picker and the built-in iPod app is only skin deep. Using the iPod, a user can build an on-the-go playlist. That playlist acts like other playlists; for example, it appears in the Playlists tab of the iPod application and it persists until the user changes or deletes it.

With the picker, a user instead specifies a *collection* of media items. The collection does not have the status of a playlist. It won't persist after the user quits your application—unless you archive it. Neither will the collection appear, under any circumstances, in the Playlists tab of the picker.

Getting Media Items Programmatically

If the media item picker doesn't provide the control you want, you can use the database access classes from this API. These classes are designed to let you create arbitrarily complex queries. You could, for example, retrieve all the songs in a particular genre whose titles include a particular word or phrase.

Using programmatic access is a two step process:

1. Configure a query.

2. Ask the query to retrieve its matching media items.

A *media query* is a description of what to retrieve from the device iPod library and how those retrieved items should be arranged. It has two properties to configure:

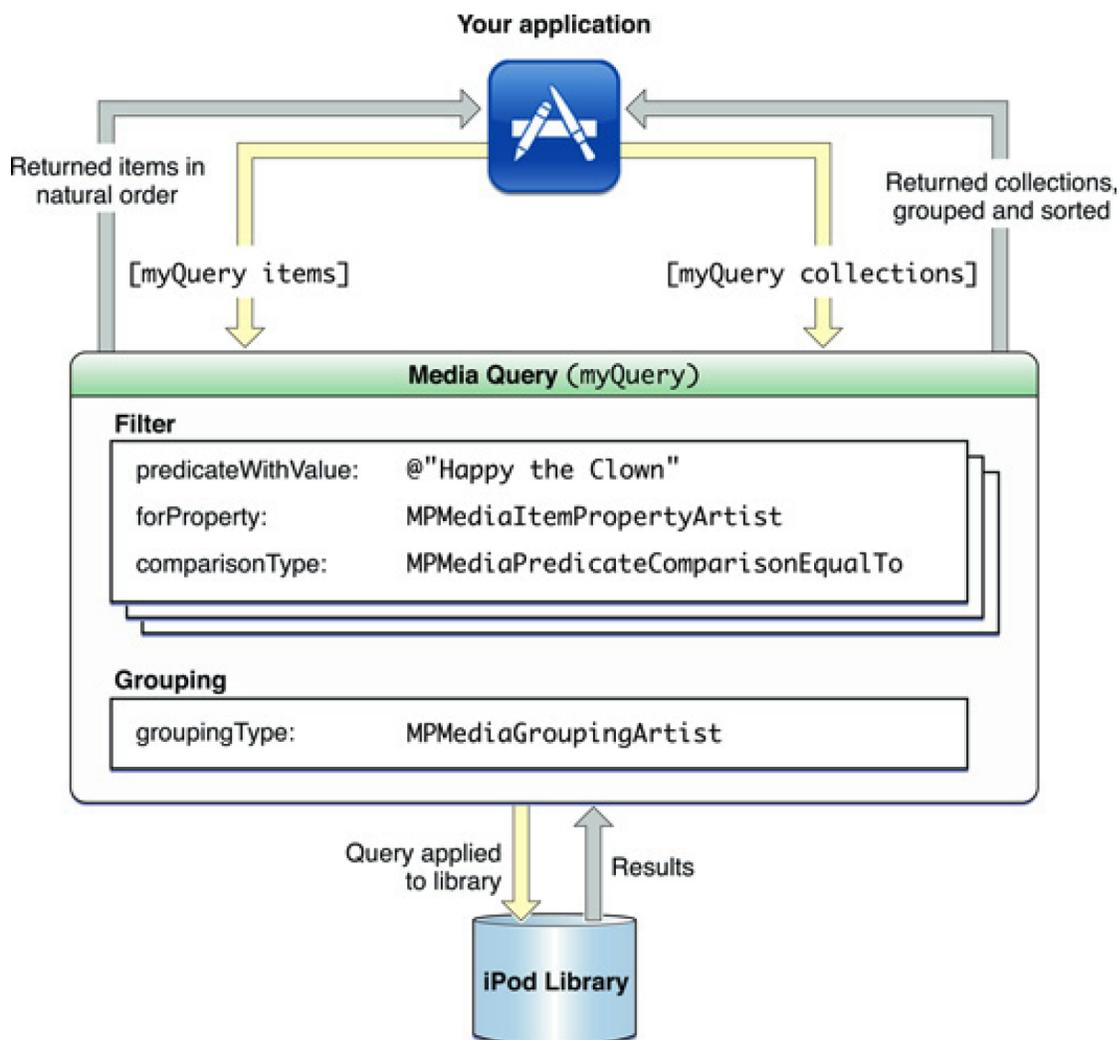
- The *filter* is the description of what to retrieve. The filter is optional; a filterless query matches the entire iPod library.
- The *grouping type* is an optional key that specifies the arrangement to use for retrieved collections of media items.

Zooming in a bit more, the filter can be as simple or complex as your application demands. It consists of one or more instances of a media property predicate. A *media property predicate* is a statement of a logical condition to test each media item against. The items that satisfy the filter are retrieved from the iPod library when you invoke the query.

The optional grouping type specifies the arrangement and sorting of collections as well as the sorting of media items within each collection. For example, using an “album” grouping type results in returned media items grouped by album, with each album’s songs sorted in track order.

Figure 1–5 shows a configured media query and its place between your application and the iPod library.

Figure 1–5 Using a media query to access the device iPod library



As the figure shows, a query can fetch items or collections.

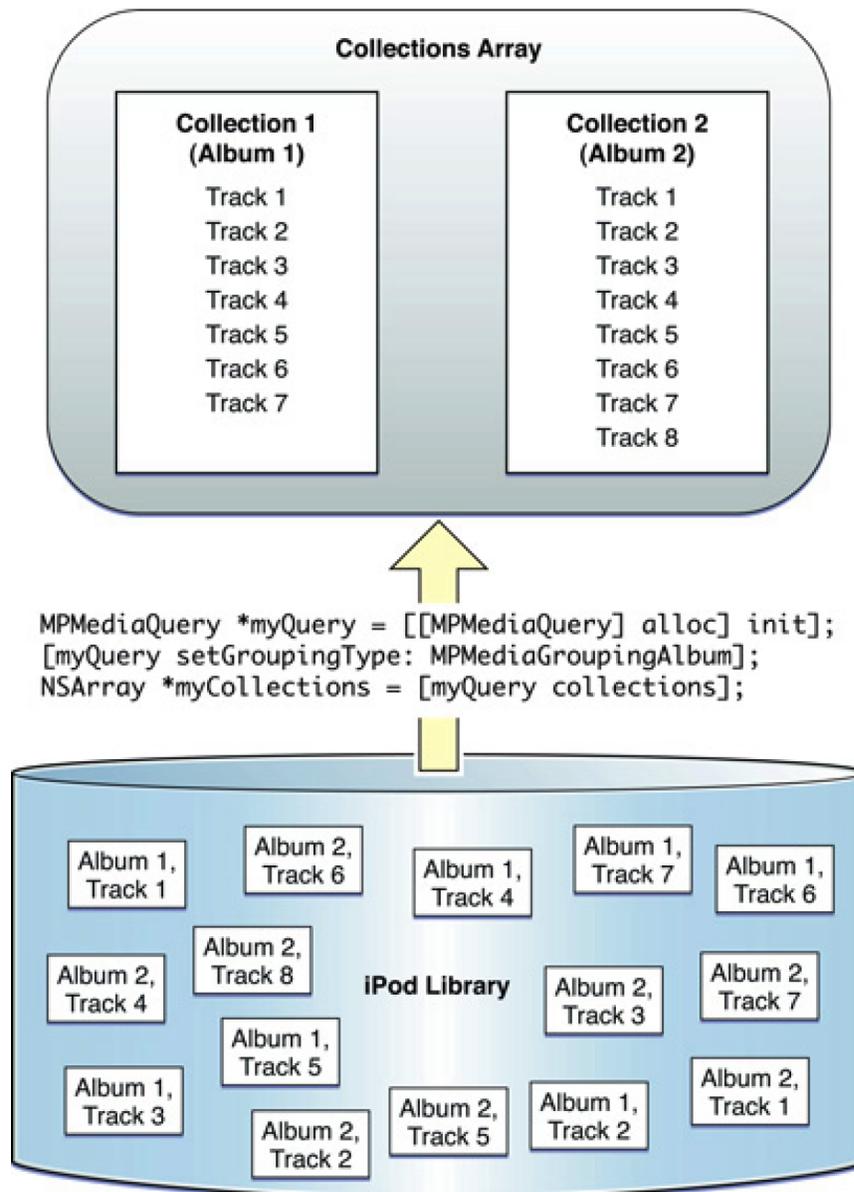
- When you ask for items, the query returns a collection containing all the items that match the filter. The items are in “natural” order, meaning that they are ordered as iTunes shows them on the desktop.
- When you ask for collections, the media query employs not only its filter but also its grouping type.

About Collections and Playlists

A *media item collection* is an array of media items. You obtain collections from the device iPod library by accessing a media query’s `collections` property. The returned value is a sorted array of collections where each collection is an instance of the query’s grouping type.

For example, say you specify an “album” grouping type by assigning the `MPMediaGroupingAlbum` key to a media query—and say that query has no filter. The value of the `collections` property is then the entire audio content of the iPod library arranged as albums, one album per collection. The collections (albums in this case) are sorted alphabetically. The songs (each a media item) within each collection are sorted by track number. Figure 1–6 illustrates this.

Figure 1–6 Obtaining collections from the device iPod library



At the bottom of the figure you see the iPod library for a device. In this illustrative case, the library has just two music albums, one with seven tracks and the other with eight. The items are in their “natural” order, as they appear in iTunes on the desktop.

The up-pointing arrow in the middle of the figure represents the definition of a generic (filterless) query, the application of the “album” grouping type, and the accessing of that query’s `collections` property.

The top of the figure represents the result of the `collections` call. It is an array whose elements are, in turn, arrays of media items. The collections array is sorted by album name. Each collection is sorted by track number.

You can construct your own collections as well. This can be useful, for example, for managing the selections a user has made with a media item picker. Note, however, that collections are not mutable.

A *playlist* is special sort of media item collection. It has properties that regular collections do not have, such as a name and a persistent ID. Playlists are created by users on the desktop; on the device they are

read-only.

Using iPod Library Change Notifications

The `MPMediaLibrary` object represents the state of the device iPod library. You can use it to ensure that your cache of the library contents is up to date. This is useful because a user may sync their device, changing the content of the iPod library, while your application is running.

Mixing Your Own Sounds with iPod Library Sounds

Note: To mix application sounds with sounds from the device iPod library, you need to understand audio sessions, audio session categories, audio hardware route changes, and audio interruptions. To learn about these, refer to *Audio Session Programming Guide*.

You also need to understand how your choice of audio formats can impact the simultaneous playback of sounds on a device. See *Playing Multiple Sounds Simultaneously* in *Core Audio Overview*.

A music player automatically employs the Media Playback audio session category. If your application uses a music player and no other sounds, you should write no audio session code. Specifically, you should not initialize, configure, or activate the audio session. The system automatically handles playback, audio hardware route changes, and audio interruptions for music players.

On the other hand, to mix application sounds with iPod library sounds, you need to configure and use your application's audio session. Employ the Ambient category to support mixing. Handle audio interruptions, audio hardware route changes, and audio session reactivation as described in *Audio Session Programming Guide*. For an example of mixing application sound with iPod sound, see the *AddMusic* sample.

EXHIBIT H

[Discover](#)[Design](#)[Develop](#)[Distribute](#)[Support](#)[Account](#)

Documentation **Apple Music API**
API Changes: [None](#)

Web Service

Apple Music API

Integrate streaming music with Apple Music content.

On This Page

[Overview](#) 

[Topics](#) 

[See Also](#) 

Overview

The Apple Music API is a web service that lets you access information about the media found in the Apple Music Catalog and the user's personal iCloud Music Library. Here's what each one includes:

- The Apple Music Catalog includes all resources available in Apple Music.
- The user's iCloud Music Library contains only those resources that the user added to their personal library. For example, it contains items from Apple Music, songs purchased from iTunes Store, and imports from discs and other apps. This library may include content not found in the Apple Music Catalog.

Use this service to retrieve information about albums, songs, artists, playlists, music videos, Apple Music stations, ratings, charts, recommendations, and the user's most recently played content. With proper authorization from the user, you can also create or modify playlists and apply ratings to the user's content.

Topics

Essentials

-  Getting Keys and Creating Tokens
Obtain developer tokens and keys needed to make requests to the Apple Music API.
-  Handling Requests and Responses
Write a request and handle a response from the Apple Music API.
-  Handling Relationships and Pagination
Fetch related objects as part of your original request and paginate the results from the Apple Music API.
-  Storefronts and Localization
Pick a country-specific geographic region from which to retrieve catalog information, or retrieve information from the user's personal library.
-  Common Objects
Understand the base types used to construct the JSON data you receive.

Albums, Artists, Songs, and Videos

-  Albums
Get an album's name, artist, list of tracks, artwork, release date, and recording information, and add new albums to the user's library.
-  Artists
Get information about an artist, including the content they created and references to them in playlists and radio stations.
-  Songs
Get information about a particular song, including the artist who created it and the album on which it appeared.
-  Music Videos
Get information about a music video, including the artist who created it and the associated album, and add new videos to the user's library.

Playlists and Stations

 Playlists

Get the contents of playlists, add new playlists to the user's library, and add tracks to an existing playlist.

 Apple Music Stations

Get information about streaming content offered by Apple Music.

Search

 Search

Search for albums, songs, artists, and other information in the user's personal library or the Apple Music Catalog.

Ratings and Charts

 Ratings

Get and set ratings for albums, songs, playlists, music videos, and stations.

 Charts

Get chart information that shows the popularity of albums, songs, and music videos.

Genres, Curators, and Recommendations

 Music Genres

Get information about the genres associated with the user's music or with items in the Apple Music Catalog.

 Curators

Get information about the person who curated a playlist or station.

 Recommendations

Get music recommendations based on the user's library and purchase history.

Activities and History

 Activities

Get the activities associated with the Apple Music Catalog.

 History

Get historical information about which songs and stations the user played recently.

See Also

Related Documentation

Media Player

Find and play songs, audio podcasts, audio books, and more from within your app.

StoreKit

Support in-app purchases and interactions with the App Store.

MusicKit JS

Add an Apple Music player to your web app.

EXHIBIT I

Andrew McAfee (<http://andrewmcafee.org>)

About (<http://andrewmcafee.org/about/>) Books (<http://www.amazon.com/Andrew-McAfee/e/B002A51606>)

Articles (<http://andrewmcafee.org/my-articles/>)

Videos (https://www.google.com/search?biw=1225&bih=1388&tbm=vid&q=andrew+mcafee+video&oq=andrew+mcafee+video&gs_l=psy-ab.3..0.4870.6021.0.6612.6.6.0.0.0.0.159.534.3j2.5.0....0...1.1.64.psy-ab..1.5.533...0i20i263k1.0.1iZeFhBlws)

Podcast (<http://andrewmcafee.org/podcast>) MIT (<http://mitsloan.mit.edu/ide/>)

Contact (<http://andrewmcafee.org/contact/>)

SpyTunes

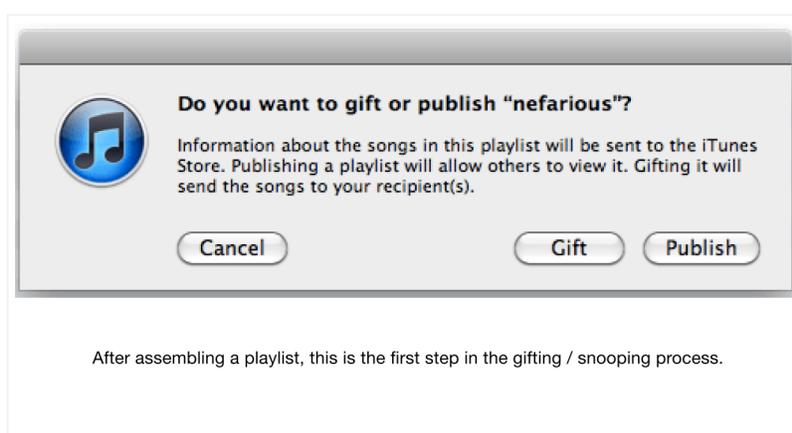
A little while back I was putting together an iTunes playlist (http://mp3.about.com/od/tutorials/ss/iTunesplist_tut.htm) to give to my Mom (<http://andrewmcafee.wpengine.com/2010/03/ada-lovelace-day-thanks-mom/>) as a gift, and found myself frustrated by the application's user interface. It kept telling me that Mom already had one song after another, and refusing to let me complete the gifting process until I removed the duplicate song from the playlist.

After I did this three or four times I gave up, complaining to my girlfriend how clunky the process was. She replied “That’s not the real problem. The real problem is that iTunes is telling you what music someone else has.”

She’s right. I’ve been doing some poking around, and have found that it’s pretty straightforward for one person (let’s call him George Smiley (<http://www.amazon.com/Smileys-People-Alec-Guinness/dp/B00007LV9M>), after John Le Carré’s (<http://www.johnlecarre.com/author/>) master spy (<http://www.guardian.co.uk/books/2009/may/22/le-carre-call-for-the-dead>)) to find out what music, video, and apps someone else (like me) has purchased or had gifted to them on iTunes.

Smiley doesn’t need to spend any money, or even have an iTunes account. He just needs a copy of the iTunes application (<http://www.apple.com/itunes/download/>) (which is downloadable and free) and knowledge of the email address associated with my iTunes account. This is often not too hard to figure out; most of us use only a few different addresses, and everything I’ll show below can be repeated over and over with every email address Smiley knows or guesses for me until he hits paydirt. So for now, let’s assume Smiley knows that my iTunes email address is my standard gmail address.

Smiley would assemble a nefarious playlist of music — the tracks he wants to determine if I own. He then starts the iTunes gifting process (I believe the maximum size for gift playlists is 100 tracks):



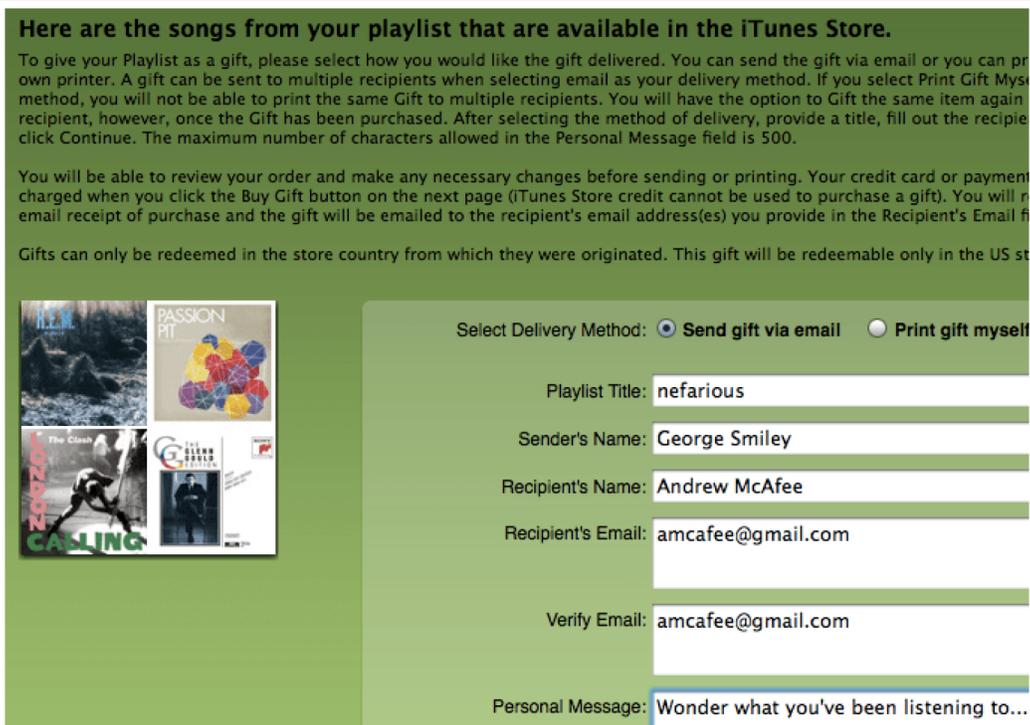
Smiley clicks ‘Gift’ and is presented with the standard iTunes screen for gifting content. He fills in the requested fields:

Here are the songs from your playlist that are available in the iTunes Store.

To give your Playlist as a gift, please select how you would like the gift delivered. You can send the gift via email or you can print it on your own printer. A gift can be sent to multiple recipients when selecting email as your delivery method. If you select Print Gift Myself method, you will not be able to print the same Gift to multiple recipients. You will have the option to Gift the same item again to a recipient, however, once the Gift has been purchased. After selecting the method of delivery, provide a title, fill out the recipient's name and email address, and click Continue. The maximum number of characters allowed in the Personal Message field is 500.

You will be able to review your order and make any necessary changes before sending or printing. Your credit card or payment method will be charged when you click the Buy Gift button on the next page (iTunes Store credit cannot be used to purchase a gift). You will receive an email receipt of purchase and the gift will be emailed to the recipient's email address(es) you provide in the Recipient's Email field.

Gifts can only be redeemed in the store country from which they were originated. This gift will be redeemable only in the US store.



Select Delivery Method: Send gift via email Print gift myself

Playlist Title: nefarious

Sender's Name: George Smiley

Recipient's Name: Andrew McAfee

Recipient's Email: amcafee@gmail.com

Verify Email: amcafee@gmail.com

Personal Message: Wonder what you've been listening to...

The snooper George Smiley tells iTunes to gift me his nefarious playlist

After Smiley clicks 'Continue,' iTunes performs a number of checks in the background. One of them is to see if the intended recipient (me, in this case) already has in his library any of the music on the playlist. This is done with good intentions — to keep users from gifting music that the recipient already has — but the implementation of this feature opens up privacy concerns: if the check reveals duplicates, iTunes tells the gifter about one of them. The application presents this information to Smiley in red ink, before he has to sign in to his account, present credit card information, or take any other steps:

Select Delivery Method: Send gift via email Print gift myself

One of your recipients (amcafee@gmail.com) has already purchased the Song "Sleepyhead".

Playlist Title: nefarious

Sender's Name: George Smiley

Recipient's Name: Andrew McAfee

Recipient's Email: amcafee@gmail.com

iTunes tells Smiley about one of the songs in my library

If he wants to explore the contents of my music library more, he deletes this song from the nefarious playlist, then resends it. He repeats this fishing expedition as often as he likes. **I have no knowledge of these activities and no way to stop them.** And the language Apple uses is not quite accurate. In the example above, I might not actually have purchased “Sleepyhead;” it might have been a gift. So Smiley’s learning about music that I didn’t even buy for myself, and might not ever have wanted.

Smiley’s technique also works for video...:



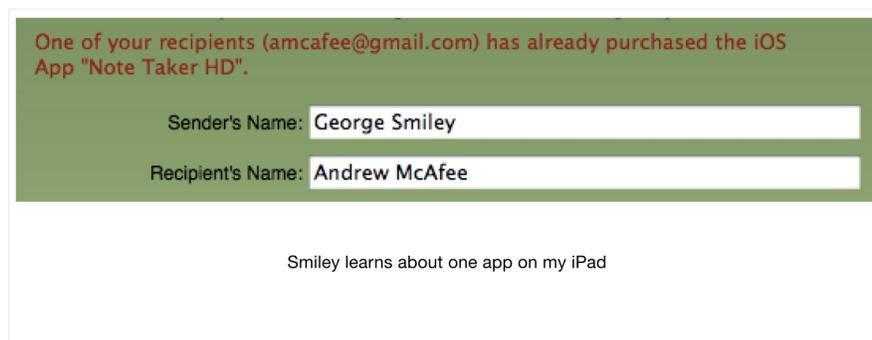
One of your recipients (amcafee@gmail.com) has already purchased the TV Season "Breaking Bad, Season 3".

Sender's Name: George Smiley

Recipient's Name: Andrew McAfee

Smiley learns about video I've purchased from iTunes

and iPhone / iPad apps that cost money:



One of your recipients (amcafee@gmail.com) has already purchased the iOS App "Note Taker HD".

Sender's Name: George Smiley

Recipient's Name: Andrew McAfee

Smiley learns about one app on my iPad

This snooping process is iterative and cumbersome, but I’m pretty sure it could be at least somewhat automated. It’s also a little fluky; to learn what I have, Smiley has to gift media to me in the same form I bought it. For example, if he sent me only a single episode of “Breaking Bad” season 3 iTunes wouldn’t send him a message like the one above. This is because I bought the whole season at once, so Smiley has to gift me the whole season to learn about my purchase. Similar rules appear to hold for music.

Even though Smiley has to work a bit, I’m not thrilled that he (or anyone else) can so easily learn about my media purchases and tastes. If I want to share my iTunes holdings with my friends or broadcast them to the world Apple gives me tools (<http://www.apple.com/itunes/ping/>) to do so, but if I want to keep them private I can’t.

This strikes me as problematic. A person's taste in media can be highly personal, yet all of Apple's more than 10 billion song and 200 million TV and movie downloads (http://en.wikipedia.org/wiki/iTunes_Store#Market_share_and_milestones) are potentially traceable by the George Smileys of the world — the world's spies, stalkers, yellow journalists, and opposition researchers. Of course, this is nowhere near as big a deal as privacy holes in online health or financial information would be, so we should keep this issue in perspective. But it is an issue, I think.

Apple's legal department will probably be particularly interested in the video example above, thanks in no small part to Robert Bork (http://www.google.com/images?q=robert+bork&um=1&ie=UTF-8&source=univ&ei=TLVdTfyKHMGC8gbn2q-ShCw&sa=X&oi=image_result_group&ct=title&resnum=3&ved=0CDgQs-AQwAg&biw=724&bih=973). During his contentious Supreme Court confirmation hearings (http://en.wikipedia.org/wiki/Robert_Bork_Supreme_Court_nomination) in 1987, much attention was focused on Bork's view that the US Constitution ensures no general right to personal privacy (<http://plato.stanford.edu/entries/privacy/>) (legal scholars, please forgive me if my language is insufficiently precise here). In a highly personal exploration of his espoused theories, the *Washington City Paper* (<http://www.washingtoncitypaper.com/>) obtained and published the list of his rentals from a Chicago video store. Congress then quickly passed a law, the Video Privacy Protection Act (<http://epic.org/privacy/vppa/>), making such publication a federal offense (many states have since passed more restrictive laws in this area).

The VPPA concerns the “wrongful disclosure of video tape rental or sales records” and states (http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00002710----000-.html) that a “video tape service provider” means any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials.” Apple might well qualify as such a provider; the act has been used as the base of class-action lawsuits against Facebook and Netflix (http://en.wikipedia.org/wiki/Video_Privacy_Protection_Act).

As a comparison, I tried to send (<http://www.amazon.com/gp/help/customer/display.html?nodeId=200375750>) my Mom an Amazon Kindle (<http://www.amazon.com/kindle-store-ebooks-newspapers-blogs/b?ie=UTF8&node=133141011>) book I knew she already had. Ama-

zon let the purchase go through and told me nothing about her Kindle inventory. She received a message from the company that I'd sent her an e-book she already owned, and giving her a credit for its price. To put it mildly, this seems like a better approach to me.

Since taking the screenshots above I've changed the email address associated with my iTunes account. I hope that brings me a bit more privacy; I don't want my fondness for Journey (<http://www.youtube.com/watch?v=TyzQl1msfnU>) becoming public knowledge...

I'm a big user of Apple products and fan of the iCcosystem they've built (see posts here (<http://andrewmcafee.wpengine.com/2010/06/my-ipad-a-great-bundle-of-sticks/>), here (<http://andrewmcafee.wpengine.com/2010/06/why-some-geeks-hate-the-ipad-so-much/>), and here (<http://blogs.hbr.org/hbr/mcafee/2010/10/in-praise-of-closed-systems.html>)). But what I've described here is a privacy hole they need to plug, fast.

Share this:

 Facebook (<http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation/?share=facebook&nb=1>)

 LinkedIn (<http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation/?share=linkedin&nb=1>)

 Twitter (<http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation/?share=twitter&nb=1>)

 Google (<http://andrewmcafee.org/2011/02/mcafee-apple-itunes-privacy-hole-violation/?share=google-plus-1&nb=1>)

© 2019 Andrew McAfee

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Apple Discloses iTunes Store App Customers' Personal Information Without Consent, According to Class Action Suit](#)
