IT'S NOT HOW MUCH DATA YOU HAVE, BUT HOW YOU USE IT:
Assessing Privacy in the Context of Consumer Data Integration

Jules Polonetsky and Omer Tene
Future of Privacy Forum

FPF

Jules Polonetsky and Omer Tene, Future of Privacy Forum[*]

This paper addresses how policymakers should think about privacy in a world where leading technology companies are increasingly providing integrated products and services across the breadth of our digital lives, using personal data for multiple purposes. We explain that consumers are unlikely to object where the use of personal data is contextually consistent or where other circumstances warrant data use for an integrated user experience. Indeed, many benefits flow from integrated services, favoring a reasoned consideration of the issue. We describe the circumstances in which new uses of data should be considered favorably, as well as those where a change in context will require action ranging from consumer communication to express consent.

INTEGRATED HARDWARE-SOFTWARE SOLUTIONS

Leading technology companies such as Amazon, Apple, Facebook, Google and Microsoft have diversified vertically into multiple market segments. Companies previously known for one or two technologies are now expanding into mobile devices; operating systems; browsers; voice, photo and video services; gaming platforms; email and messaging services; search engines; blogging platforms; storage facilities; social networks; ad networks and more.[1] In the past, Apple was uniquely situated as a provider of both hardware and software. Recently, expansion into new technologies has become the market norm, as Amazon, Microsoft and Google, once exclusively software providers, now deliver increasingly integrated services and devices. While rumors of a Facebook phone persist, Facebook remains one of the few industry giants that have not launched an integrated hardware device.[2] Rather Facebook now operates on more than 2,500 different models of mobile phones and is forging relationships with existing mobile operators.[3]

A central driver for integration has been consumer demand for smooth interoperability between hardware, operating systems, and software apps. Hence, platform expansion is a bottom-up process, where consumers' expectations lead companies to expand brand offerings into new market segments. In their recent book, *Interop: The Promise and Perils of Highly Interconnected Systems*, John Palfrey and Urs Gasser explain: "users want their computers to work seamlessly with their cameras and smartphones. Nothing drives consumers crazier in the digital economy than technology systems that will not work together properly."[4]

Apple has cemented its position as a market icon by offering a seamlessly cohesive user experience based on well-designed, fully integrated software and devices. As users have shifted from desktop to mobile platforms, Google has begun to provide a mobile experience featuring an operating system, search engine, map service, and app store.

---

[1] Technology giants at war: Another game of thrones, THE ECONOMIST, Dec. 1, 2012, http://www.economist.com/news/21567361-google-apple-facebook-and-amazon-are-each-others-throats-all-sorts-ways-another-game.
[2] *See* Annex A, Future of Privacy Forum Multiple Service Technology Companies.
[3] Jessica Guynn, After a billion, what's next for Facebook?, LA TIMES, Dec. 2, 2012, http://touch.latimes.com/#section/-1/article/p2p-73535626.
[4] John Palfrey & Urs Gasser, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS (Basic Books, 2012).

Indeed, even Microsoft, which has long adhered to a strategy of selling software for computers of every make, has now launched its own tablet and recalibrated its focus to package "devices and services."[5]

Companies without integrated solutions risk being marginalized by competitors and losing access to consumers. Consider Amazon, which launched the Kindle as its own e-reader, despite incurring steep costs, to ensure that readers of e-books had easy access to the Amazon store. The Kindle now provides Amazon with an all-important direct channel to its mobile consumers, avoiding the obligation to pay Apple or Google 30% of sales made through the Amazon app on the iPhone or Android devices.[6] Apple's recent decision to replace Google Maps with its own service and eliminate the pre-installed YouTube app further reinforces the value of Google's Android alternative.[7] Moreover, some industry observers are predicting that Apple will eventually replace Google as the default search engine on iPhones, iPods and iPads, as it has done in China. Many commentators already believe that mobile search will be based on voice recognition systems such as Siri.[8] In light of these developments, it is clear why the success of the Android platform, launched less than five years ago, is important to Google's future.

SOCIAL SEARCH

Users of social networking services are creating an increasing portion of the content available on the Internet. This content generally is off limits for search engines such as Google that crawl, index and categorize the open Web. Indeed, experts argue that the so-called "searchable Web" is shrinking, as users spend more time and energy posting content, photos, and video on Facebook.[9] Concurrently, users seek recommendations or advice less from the open Web and more from their friends on social networking services. Even outside the walled-garden of social networking services, content that has been shared or "liked" has become significant for personalization and indications of relevancy.

Facebook imposes strict limits on the collection of data by ad networks serving ads on its site. As a result, ad networks, which typically collect user data to create behavioral profiles, are limited in their access to data through the Facebook ecosystem. For all of these reasons, Google has created its own social networking service, Google Plus. At the same time, Facebook has collaborated with Microsoft's Bing to enhance the capabilities and breadth of social search.[10]

---

[5] Steve Ballmer, Shareholder Letter, October 9, 2012, http://www.microsoft.com/investor/reports/ar12/shareholder-letter/index.html.

[6] Jay Yarow, Amazon Has Found a Clever Way to Avoid Giving Apple a 30% Cut of eBook Sales — Here's How, BUSINESS INSIDER, Jan. 11, 2012, http://www.businessinsider.com/amazon-kindle-ipad-store-2012-1?op=1.

[7] Roger Kay, Removing Google Maps May Push Potential Apple Customers Toward Android, FORBES, Sept. 27, 2012, http://www.forbes.com/sites/rogerkay/2012/09/27/removing-google-maps-may-push-potential-apple-customers-toward-android.

[8] Jacqui Cheng, Siri versus Google Voice Search: Fight!, ARSTECHNICA, Nov 14 2012, http://arstechnica.com/apple/2012/11/siri-versus-google-voice-search-fight.

[9] Ben Elowitz, The Web Is Shrinking. Now What?, DIGITAL QUARTERS BLOG, June 23, 2011, http://digitalquarters.net/2011/06/the-web-is-shrinking-now-what.

[10] Lance Ulanoff, Bing Reinvents Social Search and Discovery, MASHABLE, May 10, 2012, http://mashable.com/2012/05/10/bing-social-search-discovery.

OPERATING SYSTEMS AND BROWSERS

In the past, operating systems, browsers, and hardware devices were clearly separated. Yet these boundaries are increasingly becoming blurred. Browsers play an important role in providing security by reviewing web sites against those blacklisted for infection with malware. Significantly, where cellphone operators once dictated the services available to users on their devices, these services are now provided by carriers, operating system providers, app developers, ad networks and others. The mobile operating system is shaped by consumer demand for a holistic experience and is increasingly influencing the desktop environment, with Macs and Windows 8 PCs offering app platforms. The same trend has begun to impact consumer homes, living rooms, and street behavior with the integration of gaming systems such as Xbox with online services as well as the advent of smart home devices and introduction of wearable devices such as Google glasses.

NEW SOLUTIONS; NEW PROBLEMS

Consumers are presented today with an unprecedented array of choices for integrated products and services. But that very integration means that data provided for one purpose may be re-purposed to provide a coordinated service. Journalists and privacy advocates have sounded alarm bells when companies adjusted their policies to enhance data sharing and integration.[11] Specifically, heated debates have surrounded the degree of *choice* consumers must be provided with respect to data uses; how such choices are to be made; and what the default rules should be.[12]

RESPECT FOR CONTEXT

In its report, *Protecting Consumer Privacy in an Era of Rapid Change*, the Federal Trade Commission ("FTC") determined that companies do not need to provide choice before collecting and using consumer data for practices that are "consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law."[13] As a corollary, companies should give consumers choice with respect to practices inconsistent within the context of their interaction. The focus on context is consistent with the "Respect for Context" principle in the *Consumer Privacy Bill of Rights* proposed by the White House.[14] In addition, the FTC called on companies to provide consumers with choice as to whether they will be tracked across other parties' websites.

The Respect for Context principle is derived from work by Helen Nissenbaum, who defines "contextual integrity" as "a function of several variables, including the nature of the situation or context; the nature of information in relation to that context; the roles of agents receiving information, their relationships to information subjects; on what terms the information is shared by the subject and the terms of further dissemination."[15] Nissenbaum explains that "because

---

[11] *See, e.g.*, Eric Pfanner & Kevin O'brien, Europe Presses Google to Change Privacy Policy, NY TIMES, October 16, 2012, http://www.nytimes.com/2012/10/17/business/global/17iht-google17.html.

[12] Omer Tene & Jules Polonetsky, To Track or 'Do Not Track': Advancing Transparency and Individual Control in Online Behavioral Advertising, 13 MINN. J. L. SCI. & TECH. 281 (2012).

[13] Federal Trade Commission Report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, March 2012, pp. 36-40, http://ftc.gov/os/2012/03/120326privacyreport.pdf.

[14] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Feb. 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[15] Helen Nissenbaum, Privacy as Contextual Integrity, 79 WASH. L. REV. 119 (2004). *Also see* Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (Stanford Law Books 2009).

questions about whether particular restrictions on flow are acceptable call for investigation into the relevant contextual details, protecting privacy will be a messy task, requiring a grasp of concepts and social institutions as well as knowledge of facts of the matter."[16]

This "messy task" must also take into account that relationships can and should change over time. Companies can successfully extend their brands to previously untapped markets, broadening their consumer relationships without violating consumer expectations. Some argue that soliciting express consent is a prerequisite to *any* shift in existing boundaries. In reality, however, shifting contexts are not always readily negotiated. Rather, companies should assess the effects of any prospective change on consumer expectations; convey their policies clearly and conspicuously; and in certain cases provide consumers with an opportunity to opt out. When a change in context is radical and consumer communications inadequate to support it, express consent can be relied upon to ensure that consumers are willing to accept a new data use.

In adopting the context test, the FTC modified the approach in its proposed framework, which originally set forth a list of five categories of "commonly accepted" data practices for which companies would not be required to provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing).[17] The FTC came to realize that context is not subject to hard and fast rules. Data practices and context need to be evaluated according to case-specific consumer expectations. Amazon, for example, may pursue a high degree of customization without violating consumer expectations, given its clear messaging about customization and friendly user interface; whereas Orbitz will surprise users when tailoring specific kinds of travel offers to their browser type.[18] As Nissenbaum puts it: "Although the online bookseller Amazon.com maintains and analyzes customer records electronically, using this information as a basis for marketing to those same customers seems not to be a significant departure from entrenched norms of appropriateness and flow. By contrast, the grocer who bombards shoppers with questions about other lifestyle choices—*e.g.*, where they vacationed, what movies they recently viewed, what books they read, where their children attend school or college, and so on—does breach norms of appropriateness."[19]

Under the contextual approach, data use practices are not evaluated in a vacuum. Crude criteria such as the size of a company, the number of consumers or the breadth of data under its control are not dispositive. Rather it is the context of a transaction or relationship, shaped by consumer expectations, that legitimizes data practices. In some cases, consumers may want and expect a smoothly integrative solution. In this case, prompting for permissions would be disruptive of user experience and superfluous.[20] Moreover, by clearly communicating its data policies including any purported changes, a company can help shift consumer expectations to align them with prospective data use. An individual using a device marketed by a social networking service reasonably expects such a device to be embedded with data sharing features. Consumers who used All Advantage – a dial up ISP launched in 1999 which

---

[16] Nissenbaum, *supra* note 15, at p. 156.

[17] Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, December 2010, http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[18] Dana Mattioli, On Orbitz, Mac Users Steered to Pricier Hotels, WSJ, Aug. 23, 2012, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html.

[19] Nissenbaum, *supra* note 15, at p. 152-53.

[20] Consider the effects of the EU "Cookie Directive"; Sophie Curtis, Information Commissioner Criticizes 'Dreamed up' EU Cookie Directive, TECHWORLD, Sept. 14, 2012, http://news.techworld.com/security/3381339/information-commissioner-criticises-dreamed-up--eu-cookie-directive.

provided connectivity in return for tracking users and serving pop-up ads – understood the benefit of the bargain and were not surprised by tracking.

INNOVATIVE USES

The trickiest decisions involve truly innovative data practices, which by definition cannot be anticipated by consumers. Nissenbaum posits that "by putting forward existing informational norms as benchmarks for privacy protection, we appear to endorse entrenched flows that might be deleterious even in the face of technological means to make things better. Put another way, contextual integrity is conservative in possibly detrimental ways."[21] For example, if Facebook had not proactively launched its News Feed feature in 2006 and had instead solicited users' opt-in consent, we might not have benefitted from Facebook as we know it today. It is only when data started flowing that users became accustomed to the change, which is viewed today as an indispensable service by more than a billion users worldwide. Hence even in these cases of groundbreaking innovation, opt-in consent is not always advisable.[22] Certain prospective data uses are so immensely valuable that their deployment even without prior consent is compelling. Consider the case of Dr. Russ Altman, a professor of bioengineering at Stanford, who was able to discover a harmful drug interaction by combing through Microsoft Bing search query logs.[23] For the estimated one million Americans who used to take both drugs together, Altman's work was potentially life-saving, while the privacy costs of his processing de-identified search queries limited. Another example is Comcast's decision in 2010 to pro-actively monitor its customers' computers to detect malware;[24] more recently, Internet-service providers including Comcast, AT&T, and Verizon have reached out to consumers to report that those consumers' computers had been infected and used by criminals as bots.[25] Users benefit from this approach, as do those who would be harmed by bot network attacks. Similarly, it seems clear that most consumers welcome cellphone operators' use of information to ensure quality and reliability of service.

In each of these cases – Facebook's News Feed, Altman's research, and Comcast's warning – companies may have struggled if asked to obtain individuals' prior opt in consent to data practices which were truly innovative and unanticipated. In fact, many Facebook users initially reacted negatively to the introduction of News Feed, criticizing the changed user experience.[26] Once they adjusted to this change in context, however, News Feed became a vital part of the Facebook experience, driving user engagement and playing a crucial role in spreading information globally. While each of these innovations signified a change in context that benefits consumers and perhaps society at large, it is far from clear that individuals would have opted-in to these practices if asked to do so in advance.

In a recent article concerning the costs and benefits of "big data" analysis, the authors of this paper explained: "We do not argue that individuals should *never* be asked to expressly consent to the use of their information or offered an

---

[21] Nissenbaum, *supra* note 15, at p. 143.

[22] *See* generally, Daniel Solove, Privacy Self-Management and the Consent Paradox, 126 HARV. L. REV. ___ (forthcoming 2013).

[23] Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 NW J. TECH & IP ___ (forthcoming 2012).

[24] Roy Furchgott, Comcast to Protect Customer's Computers from Malware, NY TIMES, September 30, 2010, http://gadgetwise.blogs.nytimes.com/2010/09/30/comcast-to-monitor-customer-computers-for-malware.

[25] Daniel Lippman & Julian Barnes, Malware Threat to Internet Corralled, WSJ, July 9, 2012, http://online.wsj.com/article/SB10001424052702303292204577515262710139518.html.

[26] John Leyden, Facebook mods controversial 'stalker-friendly' feature, THE REGISTER, Sept. 8, 2006, http://www.theregister.co.uk/2006/09/08/facebook_climbdown.

option to opt-out. Rather we suggest that the merits of a given data use should be debated as a broader societal issue. Does society believe that direct marketing, behavioral advertising, third party data brokering, or location based services are legitimate (or even commendable) and should be pursued? Or are these excessive intrusions that should be deterred? When making decisions about the need for individuals' consent and how it should be obtained, policymakers should recognize that default rules often prevail and are determinative of the existence of these data uses."[27] In order to facilitate and promote innovation, a certain degree of flexibility with respect to data use is key, so long as companies do not thwart consumer expectations, fulfill their transparency obligations and implement privacy by design.

INTEGRATION AND PRIVACY BENEFITS

Vertical integration, while facilitating data flows, does not necessarily entail a deadweight privacy cost. Consider how Google and Apple each determined to "sandbox" the app environment (*i.e.*, isolate untrusted programs from other software and data resources on a user's device), requiring user granted permissions before data can be accessed by apps.[28] While the desktop computing model traditionally contained no such restrictions, the latest versions of Apple's and Microsoft's desktop platforms have introduced curated and controlled app environments, providing consumers with enhanced privacy controls.[29]

In their recent critique of the data portability requirements under the proposed new EU privacy regulation, Peter Swire and Yianni Lagos focus on the risk created by regulatory mandated ecosystems that force companies to integrate with a large number of third parties.[30] Although integration between multiple service providers can be done with regard for privacy and security, the sharing of data creates risks. In their book, Palfrey and Gasser acknowledge the privacy and security costs of interoperability, but believe that the benefits outweigh the risks.

"BRANDING PRIVACY"

In his recent article *Branding Privacy*, Paul Ohm discussed "the problem of the privacy lurch," which he defined as an abrupt change made to the way a company handles data about individuals. Ohm suggests that trademarks could bridge the notice deficiency of corporate privacy practices thereby preventing "privacy lurches."[31] Ohm's approach would require every company that handles customer information to associate its trademark with a specified set of core privacy commitments, requiring a change of trademark if the company decides to depart from its initial promises. Hence, Ohm appears to view brand development as a top-down exercise where companies shape brand qualities through purposeful, legally binding commitments. In contrast, we suggest that while brand recognition has important implications for privacy law, it is in fact a bottom-up process where *users* set their expectations based on their perception of a brand. And while companies can manage their image and brand through advertising and

---

[27] Tene & Polonetsky, *supra* note 23; also see Tene & Polonetsky, *supra* note 12.

[28] Elyse Betters, Apple now requires user permission in iOS 6 before apps can access private data, 9TO5MAC, June 14, 2012, http://9to5mac.com/2012/06/14/apple-now-requires-user-permission-in-ios-6-before-apps-can-access-private-data.

[29] We recognize, in this respect, the concern expressed by Jonathan Zittrain as to whether controlled environments limit the important generativity of the Internet. Jonathan Zittrain, THE FUTURE OF THE INTERNET – AND HOW TO STOP IT (Yale University Press 2008).

[30] Peter Swire & Yianni Lagos, Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique, ___ MARYLAND L. REV. (forthcoming 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2159157.

[31] Paul Ohm, Branding Privacy, 97 MINN. L. REV. ____ (forthcoming 2013).

marketing, it is users, not businesses that inject brands with meaning. Consequently, in order to assess the legitimacy of data practices, regulators should analyze *users' expectations* rather than corporate statements.[32] In some cases, user expectations might indeed limit a new data use, but in other cases they could help support a new product or service.

The suggestion is not that recognized brands have a *de facto* license to use data in a manner that start-up businesses do not (although users may indeed endow recognized brands with more trust than unrecognized newcomers). Rather the point is that the way a brand is perceived by users will indeed provide a company with an advantage when proposing a new data use, if such use constitutes an extension of the brand that resonates with consumers. For example, a consumer's sneakers are not ordinarily expected to communicate with the consumer's phone; but if Nike sold a Nike branded smartphone, consumers would likely expect that it communicated seamlessly with their bluetooth-enabled Nike shoes. Chief Executives and Chief Marketing Officers have for generations explored the optimal way to extend their brands to additional goods and services based on existing consumer loyalty and demand. This relationship, when utilized meaningfully, must be taken into account when evaluating changes in context.

PRIVACY BY DESIGN

Finally, in addition to managing the consumer relationships to avoid Ohm's "privacy lurch," companies seeking to change context and integrate data should implement measures of privacy by design. The FTC requires companies to "promote consumer privacy throughout their organizations and at every stage of the development of their products and services." This includes measures such as data minimization, encryption, limited purposes for data use, data security, reasonable collection limits, sound retention and disposal practices, and data accuracy. Such measures are particularly salient when new uses of data are made, given that they serve to minimize potential risks created by such new uses. Consider, for example, the innovative de-identification steps and other privacy measures designed by Bering Media for its technology enabling ISPs to help serve ads based on precise geolocation data.[33]

As part of our research, we reviewed the statements that leading companies made to describe their data use practices across services and examined the nature of choices provided to consumers. We documented many of these statements and choices in Annex B.[34] Although conduct is not consistent across companies, it is clear that best practices are emerging. Companies are offering consumers a wide range of options and in many cases, providing them with choices over how their data is used.

CONCLUSION

The Future of Privacy Forum urges that the concept of *context* introduced by the FTC Final Report be broadened to provide a flexible test for assessment of novel, innovative data practices. Context, in turn, is defined not by reviewing the size of a company or scope of data collection, but rather by examining user expectations. Second, the FTC should assess the value and potential costs of proposed data uses as well as the identity of those who derive those benefits or bear the costs. A practice which generates significant benefits to many while imposing low costs on a few may be warranted even if user expectations are exceeded. Third, companies should clearly and conspicuously communicate

---

[32] Of course, when made clearly and effectively, corporate statements influence user perceptions and expectations.

[33] *See* Ann Cavoukian, Redesigning IP Geolocation: Privacy by Design and Online Targeted Advertising, October 2010, http://www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf.

[34] Annex B: Cross Service Data Integration and Consumer Choices.

to users any innovative, previously unexpected data use. When a new use is broader than expected, choice may be required. Finally, companies' brands shape context and user expectations. For example, a social networking service can be expected to promote and facilitate data sharing. And while recognized brands do not permit companies to act without restraint or accountability, they do shape users' expectations and may facilitate expansion of data practices as long as such expansions avoid a "privacy lurch."

ANNEX A: MULTIPLE SERVICE TECHNOLOGY COMPANIES (UPDATED JUNE 22, 2015)

	Apple	Google	Microsoft	Amazon	Facebook
Desktop OS	OS X	Chrome OS	Windows	-	-
Mobile OS	iOS	Android	Windows Mobile	Kindle Fire	Facebook Home (Android UI Layer)
Email Service	iCloud (pushed from source email)	Gmail	Outlook, Exchange	-	Facebook Email
Chat Service / Mobile Messaging	iMessage	Google Talk	Skype	-	Facebook Messenger
Search	Spotlight	Google Search	Bing, powers Yahoo! Search, Apple Spotlight and Siri	A9	Bing Integration, Site Search Sponsored Results
Browser	Safari	Chrome	Internet Explorer, Edge	Fire Silk Browser	-
Phone	iPhone	Nexus	Lumia	Fire Phone	-
Tablet	iPad	Nexus Tablet	Surface	Kindle Fire	-
Social Network	Facebook and Twitter Integration with iOS/iTunes	Google +	Xbox Social, Facebook integration with Bing and Windows	-	Facebook
Computer / Laptop	Mac	Chromebook	Surface Pro	-	-
App Store	App Store	Google Play	Windows Store	Amazon Appstore for Android, Fire Appstore	App Center
Photos	iPhoto, auto-backup to iCloud	Google Photos, Photo sharing on Google +, Picasa, Google Drive backup	Photos App, auto-backup to OneDrive	-	Photo sharing on Facebook, Moments, Instagram

	Apple	Google	Microsoft	Amazon	Facebook
Music/Video	iTunes	YouTube, Google Play, Video sharing on Google +	Xbox Music, Xbox Video	Prime Instant Video, Prime Music; Twitch	Integration with music services (e.g., Spotify), Video sharing on Facebook
Voice / Video Chat	Facetime	Google Hangouts	Skype	-	Facebook Video Call
Cloud Service	iCloud	Google Drive	OneDrive, Azure, HomeGroup	Amazon Cloud Drive	-
Location Service	Apple Maps, Location Service (Wi-Fi)	Google Maps, Waze, Google+ Check-in, Location Service (Wi-Fi)	Bing Maps, Microsoft Location Service (Wi-Fi)	Amazon Maps	Facebook Check-in
Voice Recognition Service	Siri	Google Now	Cortana	Alexa (Echo)	-
Payment Service	Apple Pay	Google Wallet	Microsoft Online Payment Services	Amazon Payments, Checkout	Facebook Credits
Media Streaming / Gaming Device	Apple TV	Chromecast	Xbox One	Fire TV	-
Office Suite	iWork	Google Docs, Sheets, and Slides	Office	-	-
Online Commerce	-	Google Shopping	-	Amazon Marketplace; Zappos	Facebook Marketplace, Facebook Gifts
eBook Marketplace / Reader	iBooks	Google eBooks	-	Kindle; Audible; Apps for Desktop and Mobile OS and Browser	-
Advertising Network	iAd Network	Adsense, DoubleClick, AdMob, Admeld	Yahoo!/Bing Network, Microsoft Ad Exchange	Amazon Media Group	Facebook Mobile Ad Network, Facebook Exchange, Atlas

	Apple	Google	Microsoft	Amazon	Facebook
Wearable	iWatch	Glass, Android Wear	Band	-	-
Virtual Reality	-	Cardboard	HoloLens	-	Oculus Rift
Home Control	HomeKit	Nest	HomeOS (working name)	Echo	-
Vehicle OS	CarPlay	Open Automotive Alliance	Windows Embedded Automotive, Windows 10 IoT Core	-	-
Internet Service	-	Google Fiber, Google WiFi, Project Loon	Skype WiFi	Free 3G for Paperwhite 3G	internet.org
Proxy Service	-	Google Mobile Proxy	-	-	Onavo

ANNEX B: SELECTED EXAMPLES OF CONSUMER SERVICE DATA INTEGRATION & CONSUMER CHOICES

AMAZON

"The information we learn from customers helps us personalize and continually improve your Amazon experience. Here are the types of information we gather.

Information You Give Us: We receive and store any information you enter on our Web site or give us in any other way…You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you."[1]

"Examples of information we receive from other sources include updated delivery and address information from our carriers or other third parties, which we use to correct our records and deliver your next purchase or communication more easily; account information, purchase or redemption information, and page-view information from some merchants with which we operate co-branded businesses or for which we provide technical, fulfillment, advertising, or other services; search term and search result information from some searches conducted through the Web search features offered by our subsidiary, Alexa Internet; search results and links, including paid listings (such as Sponsored Links); and credit history information from credit bureaus, which we use to help prevent and detect fraud and to offer certain credit or financial services to some customers."[2]

"On both Amazon-owned and operated sites and unaffiliated sites, Amazon displays interest-based advertising using information you make available to us when you interact with our sites, content, or services. Interest-based ads, also sometimes referred to as personalized or targeted ads, are displayed to you based on information from activities such as purchasing on our sites, visiting sites that contain Amazon content or ads, interacting with Amazon tools, or using our payment services, like Checkout by Amazon."[3]

"Amazon Silk logs aggregate browsing information – the logs are not associated with customer identities.

Amazon Silk temporarily logs web addresses – known as uniform resources locators ("URLs") – for the web pages it serves. Amazon does not associate these URLs with a customer's identity, and we keep this information for 30 days. This information is a key factor in driving Amazon Silk's speed."[4]

Choices
"Amazon offers you choices about receiving interest-based ads from us. You can choose not to receive interest-based ads from Amazon. You will still see ads but they will not be personalized. Please visit your Advertising Preferences page to learn how to set this preference."[5]

APPLE

"You may be asked to provide your personal information anytime you are in contact with Apple or an Apple affiliated company. Apple and its affiliates may share this personal information with each other and use it consistent with this Privacy Policy. They may also combine it with other information to provide and improve our products, services, content, and advertising."[6]

"We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

• We may collect information such as occupation, language, zip code, area code, unique device identifier, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising."[7]

 "Customers also may opt-out of location-based advertising by toggling the device's location-based service capabilities to 'Off.' For customers who do not toggle location-based service capabilities to 'Off,' Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer."[8]

"Apple intends to retain the zip code information it has collected for six months to administrative and improve the iAd network. After six months, the information may be aggregated for administrative purposes."[9]

Choices
"Apple and its partners use cookies and other technologies in mobile advertising services to control the number of times you see a given ad, deliver ads that relate to your interests, and measure the effectiveness of ad campaigns. If you do not want to receive ads with this level of relevance on your mobile device, you can opt out by accessing the following link on your device: http://oo.apple.com...This opt-out applies only to Apple advertising services and does not affect interest-based advertising from other advertising networks."[10]

FACEBOOK

"We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, we may use the information we receive about you:

- as part of our efforts to keep Facebook products, services and integrations safe and secure;
- to protect Facebook's or others' rights or property;
- to provide you with location features and services, like telling you and your friends when something is going on nearby;
- to measure or understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
- to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
- for internal operations, including troubleshooting, data analysis, testing, research and service improvement.

Granting us this permission not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways."[11]

"We receive data when you visit a site with a social plugin. We keep this data for 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you."[12]

Choices
"Facebook Ads are sometimes paired with social actions your friends have taken. For example, an ad for a sushi restaurant may be paired with a news story that one of your friends likes that restaurant's Facebook page…When you show up in one of these news stories, we will only pair it with ads shown to your friends. If you do not want to appear in stories paired with Facebook Ads, you can opt out using your 'Edit social ads' setting."[13]

"When you delete an account, it is permanently deleted from Facebook. It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days. You should only delete your account if you are sure you never want to reactivate it."[14]

GOOGLE

"We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads."[15]

"Many websites, such as news sites and blogs, partner with us to show ads to their visitors…Your interests are associated with an advertising cookie that's stored in your browser. If you don't want us to store your interests, you can opt out below. Your ads preferences only apply in this browser on this computer. They are reset if you delete your browser's cookies." [16]

"In Gmail, ads are related to the content of your Google Account…No email content or other personally identifiable information will be provided to advertisers. We provide advertisers only aggregated non-personal information such as the number of times one of their ads was clicked."[17]

"We are always looking for more ways to deliver you the most useful and relevant ads - for example, we may use your Google search queries on the Web, the sites you visit, Google Profile, +1's and other Google Account information to show you more relevant ads in Gmail.

"Ad targeting in Gmail is fully automated, and no humans read your email or Google Account information in order to show you advertisements or related information."[18]

"The +1 button isn't used to track your visits across the web. Google doesn't keep a persistent record of your browsing history as part of the process of showing you a +1 button or otherwise use the fact that you personally have visited a page with the +1 button. Google may keep some information about your visit, usually for about two weeks, to maintain and debug its systems. This information isn't organized by individual profiles, usernames, or URLs".[19]

Choices
"The Ads Preferences Manager is a Google site where you can manage settings associated with the ads you see. Our goal is to provide you with transparency and choice about the ads we show you. For Google search and Gmail, we explain why you got specific ads, and we also let you block ads from websites you aren't interested in. For websites that have partnered with Google to show AdWords ads, we show you a list of interests we associate with you that can affect the ads you see on those websites. We also let you edit your interests or opt out of interest-based ads entirely."[20]

"If you don't want to see personalized ads on Google search, you can opt out. If you do this while you're signed in to your Google Account, you'll be opting out of personalized ads on both Search and Gmail, as well as ads on Google search that are customized for your browser. When you're signed out of your Google Account, you can also opt out of Google search ads that are customized for your browser; however, you'll still see ads that are personalized to your Google Account."[21]

MICROSOFT

"Microsoft uses the information we collect to operate, improve and personalize the products and services we offer. Information collected through one Microsoft service may be combined with information collected through other Microsoft services to give you a more consistent and personalized experience in your interactions with us. We may also supplement this with information from other companies. For example, we may use services from other companies to help us derive a general geographic area based on your IP address in order to customize certain services to your geographic area."[22]

"MSN Hotmail does not use the subject or text body of customers' emails for text-based targeted advertising. MSN Hotmail advertisements are based on demographic information the user provides when creating their Hotmail account, such as age, gender, language, zip code, and country."[23]

Choices
"If you don't want to see personalized ads from Microsoft, you can choose not to receive these types of ads on websites that use the Microsoft Advertising Platform by selecting the opt-out choice on this page."[24]

"At Microsoft, we do our best to provide personalized ads that you might find interesting. We don't always get it right, though. With our My Interests tool, you can help us customize your personalized ads by selecting areas that are of interest and not of interest to you."[25]

---

[1] Amazon Privacy Notice, last updated April 6, 2012, http://www.amazon.com/gp/help/customer/display.html?nodeId=468496.
[2] *Id.*
[3] Interest Based Ads, http://www.amazon.com/b/?&node=5160028011, (accessed November 16, 2012).
[4] Amazon Response to The Honorable Edward J. Markey, November 3, 2011, at 1. http://www.scribd.com/doc/75329136/Amazon-Response-11-03-11.
[5] Interest Based Ads, *supra* note 3.
[6] Apple Privacy Policy, last updated May 21, 2012, http://www.apple.com/privacy/.
[7] *Id.*
[8] Apple Response to The Honorable Edward J. Markey, July 12, 2010, at 9. http://www.wired.com/images_blogs/gadgetlab/2011/04/applemarkeybarton7-12-10.pdf.
[9] *Id.* at 12.
[10] *Id.*
[11] Facebook Data Use Policy, last updated June 8, 2012, http://www.facebook.com/full_data_use_policy.
[12] *Id.*
[13] *Id.*
[14] *Id.* You can delete your account at: https://www.facebook.com/help/contact.php?show_form=delete_account, (accessed November 16, 2012).
[15] Google Privacy Policy, last updated July 27, 2012, http://www.google.com/policies/privacy/.
[16] *See* Google Ads Preferences Manager, www.google.com/ads/preferences/
[17] Ads in Gmail and Your Personal Data, http://support.google.com/mail/bin/answer.py?hl=en&answer=6603, (accessed November 16, 2012).
[18] http://support.google.com/mail/bin/answer.py?hl=en&answer=6603, (accessed November 16, 2012).
[19] http://support.google.com/plus/bin/answer.py?hl=en&answer=1319578, (accessed November 16, 2012). Users can opt-in to enable +1 on non-Google sites to "see recommendations from people you know when you view the same content that they've +1'd." http://support.google.com/plus/bin/answer.py?hl=en&answer=1152622, (accessed November 16, 2012).
[20] Ad Preferences Manager overview, http://support.google.com/ads/bin/answer.py?hl=en&answer=2662856&topic=2662508&ctx=topic, (accessed December 3, 2012).
[21] Ads on Google search, Gmail and certain other websites, http://support.google.com/ads/bin/answer.py?hl=en&answer=1634057, (accessed December 3, 2012).
[22] Microsoft Online Privacy Statement, http://www.microsoft.com/privacystatement/en-us/core/default.aspx?PrintView=true, (last updated July 2012).
[23] Loose Wire Blog, "Hotmail, Yahoo Deny Scanning Emails," http://www.loosewireblog.com/2004/05/hotmail_yahoo_d.html, (May 6, 2004). See also, Shaw, Frank, Gone Google? Got Concerns? We Have Alternatives, Microsoft Blog, February 1, 2012. http://blogs.technet.com/b/microsoft_blog/archive/2012/02/01/gone-google-got-concerns-we-have-alternatives.aspx.
[24] Personalized Advertising from Microsoft, last updated February 2012, http://choice.live.com/advertisementchoice/.
[25] *Id.*