OPINION

The Fair Price Privacy Act: Empowering Consumers to Regulate Data Sharing through a Micropay Audit Trail Maintained by Information Fiduciaries

David Reardon, PhD
Qix Information Technology, St. Louis MO

Audit trails; Consumer protection; Data collection; Data protection; Data subjects' rights; Fiduciaries; Privacy

Introduction

Advances in information technologies are a main driver of modern economic activity. The collection and dissemination of data from personal electronic devices creates wealth for countless internet companies, manufacturers, financial institutions and telecommunications companies.

At the same time, consumers are increasingly concerned about data breaches and the misuse of personal information that goes beyond the bounds of their personal preferences. In addition, there is evidence that most people believe they should receive a share of the monetary value of their data.[1] As a result, there is a growing tension between businesses' desire for data and consumers' desire for better control over their data and privacy.

The urgency of these issues is magnified by the increasing proliferation of smart devices with microphones and cameras. These devices have a virtually unlimited capacity to capture conversations and other activity within homes and businesses. New regulations are needed, as Kaminski et al. have noted, because the makers of these devices should be required to "give notice of surveillance, to make and keep their promises, and to avert their eyes."[2]

In the United States, there are already some laws governing data privacy. For example, the Health Insurance Portability and Accountability Act (HIPPA) regulates data use and dissemination among health care providers. Similarly, the Fair Credit Reporting Act (FCRA) limits the use of data handled by consumer reporting agencies. But neither set of regulations applies to electronic manufacturers and information services that may collect health or economic data through browsers, smart speakers, or other consumer electronics.[3]

The European Union has some of the most stringent data privacy laws in the world. These were developed around the Organisation for Economic Co-operation and Development's (OECD) eight Fair Information Practice Principles (FIPPS). Broadly summarised, these eight principles comprise:

(1) limits on the collection of personal data;
(2) relevance of the data to the purposes they are necessary;
(3) explanation of the purposes when the data is collected;
(4) limiting use of the data to the purposes as previously specified;
(5) protection of the data from unauthorised use;
(6) openness regarding practices and policies regarding use of the data;
(7) a right of individuals to identify, monitor, challenge and rectify data collected about him or her; and
(8) corporate accountability for complying with the aforesaid principles.[4]

.

In light of advances in robotics and smart speakers which open new avenues of data collection, Kiminski et al. have recommended the expansion of FIPPS with ninth and tenth principles: (9) honest anthropomorphism through which a device provides better feedback to users

[1] Sarah Spiekermann, "Privacy Property And Personal Information Markets. Acatech-Deutsche Academie Der Wissenschaften" (2012); Christina Aperjis and Bernardo A. Huberman, "A Market for Unbiased Private Data: Paying Individuals According to their Privacy Attitudes", (2012) 17 First Monday 1–9, available at *http://firstmonday.org/ojs/index.php/fm/article/view/4013/3209* [Accessed 27 June 2019]; Juan Pablo Carrascal, Christopher Riederer, Vijay Erramilli, Mauro Cherubini and Rodrigo de Oliveira, "Your browsing behavior for a Big Mac: Economics of Personal Information Online", (2013) Proc. 22nd Int. Conf. World Wide Web 189–200, available at *http://arxiv.org/abs/1112.6098* [Accessed 27 June 2019].
[2] Margot E. Kaminski, Matthew Ruebe, Cindy Grimm and William D Smart, "Averting Robot Eyes", (2017) 76 Maryl. Law Rev. 983–1024, available at *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002576*. [Accessed 27 June 2019]
[3] Jack M Balkin, U C Davis and L A W Review, "Information Fiduciaries and the First Amendment Amendment", (2016) 49 UC Davis Law Rev. 1185–1234; Ariel Dobkin, "Information Fiduciaries In Practice: Data Privacy And User Expectations", (2018) 33 Berkeley Technol. Law J. 1–49; Kaminski et al., fn.2, above.
[4] Organisation for Economic Co-operation and Development, "OECD Guidelines On The Protection Of Privacy And Transborder Flows Of Personal Data", *http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#guidelines* [Accessed 27 June 2019].

regarding what data is being collected and how it is used; and (10) dynamic feedback from a device notifying users when data is being collected in order to provide an opportunity for consumer to limit the use of the data.[5]

The importance of these principles is underscored by Keats Citron and Pasquale, especially in regard to how big data can be used to score (sometimes inaccurately) a user's credit value, employment value, health and other metrics in ways that may prejudice their access to important services.[6] They make a convincing argument that that there must be guarantees for due process which can only be assured when consumers have reasonable access to audit trails and a means to challenge the accuracy of data and the algorithms used to process it.

Another significant proposal has been the suggestion by Balkin that data collectors may have a fiduciary responsibility toward the individuals about whom they have repositories of data.[7] The law already recognises that lawyers and doctors have fiduciary responsibilities regarding the data collected and held on behalf of their clients. This same concept could be extended to companies that collect repositories of data regarding their own customers, clients, users and employees.[8]

The idea of attaching fiduciary responsibilities to data (especially data collected through consumer electronics about individuals and families) is fundamentally grounded in the argument that individuals have a privacy and ownership rights that extend to the data that describes and that represents their personhood and their activities as monitored by electronic devices. Clearly, while individuals may agree to trade their data in exchange for wanted services or even remuneration, that trade is only meaningful and truly voluntary when individuals can (1) monitor and evaluate the use of their data, and (2) withdraw or modify the terms of their consent in order to limit data use to their varying needs and preferences.

The purpose of this article is to outline legislation that could achieve these ends in a fashion that creates a baseline for consumer privacy rights, while also leaving ample room for technological innovations. I have titled the outlined legislation the Fair Price Privacy Act (FPPA) to underscore the idea that consumers' fiduciary rights in regard to their data includes a right to a "fair" valuation of that data, not only at the moment it is collected but also under changing circumstances in the future.

In brief, this proposed legislation would require large data aggregators (specifically those who use or disseminate data on behalf of third parties) to provide consumers with (1) a means to access an audit trail regarding when and how their data is used by third parties; (2) a micropay credit (at minimum one one-thousandth of a cent) each time the data is used for the benefit of third parties; and (3) a means to modify the required micropay credit for use of their data.

As discussed below, numerous benefits flow from these requirements. They would provide means for individuals, scholars, privacy advocates, and advertisers to understand and audit the collection, use, dissemination and valuation of personal data. At the same time, the FPPA provides ample room for technological innovation and will directly stimulate new opportunities to expand and develop micropay economies that will benefit consumers, content creators, advertisers, data aggregators, and tax collectors.

The Fair Price Privacy Act (FPPA)—a proposal in rough draft

Definitions

A "data aggregator" is any company with annual revenue over two-million dollars which holds data associated with over five million people which is sold to or used for the benefit of third parties.

Audit trail and remuneration requirements

Any data collected by data aggregators regarding persons using or observed by electronic devices can only be disseminated to or used for the benefit of third parties when all of the following conditions are true:

(a) the person (or the owner of the electronic device, if the person associated with the data is not linked to a known user account) is provided with means to access a complete electronic audit trail identifying each transfer or use of the data for the benefit of third parties, wherein the audit trail includes:
   a. the date and time of use,
   b. identification of the third party,
   c. a summary of the use (for example, a link to an archived advertisement that was displayed),
   d. and an accounting of the credits made to a financial account assigned to the associated person (or device owner), wherein the financial account is either (1) maintained by the data aggregator for the benefit of the person, or (2) maintained by another institution or in a financial instrument, such as a blockchain, agreeable to both parties;

(b) each transfer of data, or use of the data for the benefit of a third party, shall result in a credit at a default rate of not less than one-thousandth of a cent;

[5] See Kaminski et al. (2017), fn.2, above, at 1005.
[6] Danielle Keats Citron and Fank Pasquale, "The Scored Society: Due Process for Automated Predictions", (2014) 89 Washingt. Law Rev. 1–33.
[7] See Balkin, Davis and Review (2016), fn.3, above.
[8] See Aperjis and Huberman (2012), fn.1, above; Balkin, Davis, and Review (2016), fn.3, above.

(c) the person (or device owner) is provided an electronic means to adjust the default rate (or a schedule of rates) in a range from zero to at least one thousand dollars; and

(d) any fees required by the person (or device owner) to withdraw or transfer the accumulated credits from a financial account maintained by the data aggregator shall not exceed five dollars per transaction.

Discussion

A core concept underlying the FPPA is the idea that individuals irrevocably retain some share in the ownership of the data associated with their own identities. While data aggregators may collect this data and assert some ownership over it, it is a shared ownership. They do not have unlimited rights to use it any fashion. They are information fiduciaries. They owe specific fiduciary duties to the individuals about whom the data is collected.

The purpose of the FPPA, therefore, is to spell out the specific rights retained by the individuals about whom the data is collected. Generally speaking, these include: (1) the right to monitor how their data is being used through an audit trail; (2) the right to be credited, if desired, at least a one-thousandth of a cent each time their data is transferred to or used for the benefit of a third party; and (3) the ongoing right to adjust the level of monetary compensation required for future uses of their data depending on each individual's own preferences over time.

Through these provisions, the FPPA provides a general framework to resolve most data privacy issues. Why? Because when individuals receive compensation each time their data is used, at rates they themselves have agreed to, the terms of that agreement are being ratified with each transaction. Any dissatisfaction can be remedied by adjusting one's rates, even to the point of setting the rate to a prohibitive amount.

By attaching even a nominal amount to each transaction, advertisers can be assured that data aggregators are delivering their ads in a manner that demonstrates respect for the privacy rights of their prospects and customers. And as recipients of a small payment each time they see an ad, consumers are more likely to feel respected than annoyed. If they still feel annoyed, they only need to raise their rates until the annoyance abates.

Moreover, the process of comparing what advertisers are willing to pay to target specific group of users with the amount required by individuals in that group can be automated in a way that gives greater efficiencies to both advertisers and consumers. The most ad-resistant consumers are most likely to price themselves out of seeing ads, which would be a savings for advertisers. Conversely, by tracking which consumers are most responsive to ads in a specific category, and at what price they welcome seeing such ads, data aggregators can help advertisers to optimise response rates per ad dollar.

Allowing individuals to participate in the valuation of their own data, time, attention and screen space resolves most big data privacy issues precisely because it resolves the question of whether or not individuals anticipated or agreed to their data being used in certain ways—especially when individuals are given an ongoing opportunity to modify the terms of their data use. Under the FPPA, most questions regarding data privacy are essentially re-classified as a questions regarding accuracy of accounting. Examining accounts may be tedious, but reading a balance of credits is not. While most individuals have no patience for reading and understanding the complicated terms of use agreements for Facebook, Google, and other data aggregators, most would have no trouble understanding how much they have earned for co-operating in the collection, dissemination, and valuation of their data.

Exclusions from providing audit trails

It should be stressed that, under the FPPA, companies collecting data for their own internal use and marketing are not required to provide audit trails or compensation for use of the data. These requirements apply only to personal data transferred to, or used for the benefit of, third parties, such as advertisers.

In addition, small data aggregators (including most start-ups) are exempt from the burden of maintaining audit trails and setting up a compensation system. The proposed exception for companies with under 5 million users and revenues under $2 million can obviously be adjusted to fit public policy goals. This exemption, as presented, simply illustrates how easy it would be to reduce data compliance hurdles for the small companies that are often the seedbeds for major technological innovations.

Identification to assert shared ownership

The Fair Price Privacy Act (FPPA) attaches specific rights to "the person (or the owner of the electronic device, if the person associated with the data is not linked to a known user account)" relevant to the "data regarding persons using or observed by electronic devices that is collected by data aggregators".

Preferably, the rights are attached to individual persons. But often the identity of a person may not be known—or at least not claimed until such time as the person may register his or her identity with the data aggregator. In the absence of a known person, the secondary right to access the audit trail and any remuneration should belong to the owner of the electronic device. The importance of this provision is evident in the example of minors using a shared family computer. In another example, a computer in a public library may be used by data aggregators to create a mixed user profile specific to that machine or library, but not to any particular individual. In such cases, it makes sense that the library is then the party having the rights defined by the FPPA. On the other hand, if a person

using a public computer logs into the services of a data aggregator, and therefore is identifiable, then the data can and should be assigned to that individual.

Notably, once individuals actually register their own identities with data aggregators, it is reasonable that they could then give the data aggregators the right to collect information about them from electronic devices that are not their own. For example, the image and voice recognition capabilities if electronic devices at a friend's house, a grocery store or other public venues may capture useful information that can then be accurately associated with individuals who do not own these devices. But if data aggregators can identify specific persons, they can then verify whether these persons have given permission to use data collected about themselves from any device. If such permission has been granted, that is a fair exchange under the FPPA.

Also, while the FPPA requires data aggregators to track the micropay credits owed to each person (or device owner), these credits cannot actually be claimed until the person (or device owner) registers his or her account with the data aggregator. It is likely that many users may not bother to ever register or claim their "fair share". Moreover, at the nominal rate of only one-thousandth of a cent, it would take 5,000 uses of data before a person would have $5 in credits, the point at which the funds must be available for transfer or withdrawal. Below that threshold, a company could recapture the credits through transfer fees. This provision creates another opportunity for companies to become profitable before they are faced with a requirement to actually distribute any payments.

When distributions are made, these can be through traditional means such as through ACH bank transfers, gift cards or even "in-store credits" to purchase goods or services (such as apps or game play) offered by the data aggregators themselves. Most probably, however, these credits would be distributed through one or more blockchain-based cryptocurrencies. The likelihood of this option, and the multiple benefits it provides to data aggregators, advertisers, content creators and consumers, will be examined in a later section.

Benefits of audit trails

Any meaningful regulation of data privacy requires audit trails. The question is how to balance the protection of individual privacy rights with a desire to maximise the value of personal data to the benefit of both businesses and individuals.

The current problem is that most data aggregators resist transparency. The lack of unambiguous audit trails creates suspicion in the minds of both consumers and advertisers.[9]

Left to their own devices, data aggregators would prefer to offer only a black box service: advertisers deposit money and ads are delivered. They want advertisers and consumers to trust them based on the results of their services only. But they are hesitant (1) to fully document for advertisers who is actually seeing their ads, and (2) to fully document for consumers when and how their data is being used.

Without complete audit trails, there is no real accountability, to either advertisers or consumers. Indeed, advertisers have long been concerned about their inability to monitor digital advertising waste, to verify delivery claims and to measure the efficiency of ad dollars spent to reach specific groups of people.[10]

In fact, the raw data required to provide the FPPA mandated audit trails is already being created and retained by data aggregators to facilitate data mining, profiling and the billing of advertisers. But this data is rarely, if ever, fully shared with either advertisers or individual users.

The FPPA requires data-sharing with the individuals, but it is silent with respect to advertisers. It would be reasonable to require logs to be shared with advertisers. Ideally, these would include an anonymised user code that could be matched to individual audit trails of employees, test accounts or audit trails purchased from a representative sample of consumers. Through this means advertisers could verify that their ads are actually being delivered to the people intended, and run other analyses to maximise the efficiency of their ad dollars.

Because FPPA-required audit trials would assist both advertisers and consumer privacy advocates with a means to actually monitor and verify how data is being used, the accuracy of these audit trails is likely to be guaranteed without significant governmental oversight. Why? It is because the FPPA sets a default value of one-thousandth of a cent on each use of user data for the benefit of third parties. This is a small amount per use, but it is more than enough to support enforcement opportunities through class action law suits—one of the strongest incentives for compliance.

Benefits from adjustable rates

Most data privacy proposals are limited to allowing users to opt in or opt out. But that all-in or all-out approach fails to address the reality that most people would probably prefer to be partially in and partially out, depending on particular circumstance. Giving individuals a means to assign a monetary value to various uses of their data is a way for them to be partially in and partially out that is customisable to each individual, and even to a variety of different circumstances.

The FPPA, as outlined above, does not require data aggregators to provide users with a means to set different rates for different commercial categories, or for different kinds of use (email, texting, display ads, surface mail, smart speaker or TV ads, etc.). Mandating multiple rate options would be complex and would be likely to stifle innovation.

[9] Sapna Maheshwari, "He Buys a Lot of Ads, and He's Frustrated With Digital", *New York Times*, 9 April 2017, available at *https://www.nytimes.com/2017/04/09/business/media/marc-pritchard-procter-gamble-digital-advertising.html* [Accessed 27 June 2019].
[10] See above.

Moreover, a legal requirement for multiple rate options is probably unnecessary since market forces are likely to move data aggregators in that direction without any legal mandates. After all, it seems self-evident that most consumers would place a different value on different ads and different uses of their data. For example, some people may wish to charge nothing for the use of their data when receiving solicitations from charities, and a nickel to receive ads associated with a favorite hobby, and a dollar for ads related to life insurance.

In addition, when a consumer begins to feel that he or she is seeing too many ads in a certain category, they may want to increase their rate for that category in order to stem the flow of ads except from those advertisers who most value their time and attention. Alternatively, some users may choose to modify their rates in a manner designed to maximise their income from data use. But, since advertisers will have more data on who is actually responding to ads in each category, they will be in a better position to avoid sending ads to those people who look but never buy. In other words, the flow of data does not only benefit consumers. It will also benefit advertisers by giving them more ways to avoid wasting dollars on fake user accounts that do not actually generate any sales.

In short, it seems likely that market pressures to compete for the co-operation and loyalty of consumers in regard to data collection and the optimisation of ad targeting will lead data aggregators to compete in offering consumers increasing options for managing their rate schedules.

Benefits to advertisers and consumers

In short, time is money. People resent having their time wasted on spam. Conversely, they appreciate seeing ads that contribute real value to their lives.

There are two ways in which seeing ads can produce value. They can provide information that is useful, wanted or at least entertaining. Or an ad can come with a premium reward that makes the time spent on the ad worth one's time. Ideally, an ad should have both kinds of value, which is why premium rewards and free trials are so popular in advertising.

While no one can ever guarantee that every digital ad will be useful or entertaining, every ad can be associated with a premium reward under the provisions of the FPPA. This is actually beneficial to advertisers in many ways.

While the bulk of ad dollars may still go the data aggregators and ad delivery platforms, the fact that even a small portion goes to the people who sees the ads turns every ad into a premium ad—which always improves receptivity. When people know that they are getting paid for their time and attention, any annoyance at seeing ads is diminished. If any annoyance remains, the person only needs to up his rate for seeing such ads.

In short, the FPPA provides a starting point for consumers and advertisers to automate a process for negotiating a fair price on each consumer's time, attention, screen space and good will. Indeed, the advertisers who are most generous in paying more are likely to receive more engagement with their ads. They may even have more success by moving prospects through the multiple steps in a sales process with additional micropayments at each step.

The benefits to consumers are even more obvious. First, consumers will receive a steady stream of micropayments associated with the use of their data. Instead of feeling exploited by data aggregators and targeted by an endless stream of advertising, they feel engaged and rewarded as partners in the use and valuation of their time and data. Secondly, instead of having a vague unease about how their data is being collected, knowing that they have an opportunity to review their audit log, or even if they never do, knowing that there are data privacy investigators, academics and lawyers out there who are studying the accuracy of audit logs, will reduce the fear of privacy violations.

Not all users will engage. Not all will claim their micropayments. Even fewer will keep a close eye on their audit trails. But the mere opportunity to view audit trials and to modify rates when they are seeing too many ads, or alternatively, when seeking to maximise their income from data-sharing, will help users to feel more empowered, less exploited and less concerned about big data violations of their privacy.

Benefits to data aggregators and content providers

Data aggregators are well aware of the consumer push-back related to data privacy. They seem resigned to the fact that some regulatory standards are necessary, but they would mostly prefer one international standard rather than a hodge-podge of regional standards.[11] The FPPA could satisfy that concern. Indeed, if data aggregators roll it out in one country, it would be reasonable for them to apply it to all countries.

At first glance, however, it would appear that the FPPA would have a negative impact on data aggregator profits. Sharing ad dollars with consumers would appear to reduce the ad dollars available to the aggregators. But, on further examination, the FPPA may actually increase the profit opportunities for data aggregators.

First, it should be noted that micropay incentives are a popular marketing device. The same people who are glad to get reward points (micropay rewards) for using a credit card, or flying a particular airline, would rapidly embrace another system for receiving their "fair share" of marketing dollars in exchange for their time, attention and co-operation in the collection and dissemination of their marketing dollars.

[11] Arjun Kharpal, "Google's policy chief calls for "common rules" globally for tech regulation", CNBC, (10 February 2019), available at *https://www.cnbc.com/2019/02/10/google-policy-chief-tech-regulation-global-common-rules.html* [Accessed 10 July 2019].

By giving consumers their "fair share" of marketing dollars for the use of their data, consumers will naturally begin to feel like partners with the data aggregators, rather than simply the exploited masses. As partners who share in the rewards generated by their data, users will be more inclined to provide access to more data about themselves, because more data will help them earn more micropayments. Sensitivity regarding the collection and use of real-time GPS data, iBeacon in-store activity, bank records, health records and even DNA results is likely to decline as consumers begin to see opportunities to earn more credits for sharing more data. So it is likely that the FPPA will improve the ability of data aggregators to gather more valuable data, which in turn should increase both efficiency and earnings.

Indeed, if aggregators encourage consumers to create schedule rates required to receive ads in different commercial categories, that schedule of rates is itself useful data for the targeting of ads. Moreover, data aggregators will be able to collect additional fees on tiered marketing campaigns. With the opportunity to give micropay incentives to prospects (such as an extra 5 cents to watch a video, or 20 cents to complete a survey, or a dollar to join an email list), advertisers are likely to increase their spending on more highly targeted campaigns. At each step, data aggregators can collect additional fees.

Perhaps the greatest opportunity for data aggregators to increase revenue under the provisions of the FPPA, however, is through financial exchange fees between consumers and content providers. While the FPPA caps exchange fees to being no more than $5 per transaction, in practice it is reasonable to expect that fees of up to 30 per cent or more could be levied on billons of micropay transactions between consumer accounts, content creators and online services.

This is where the micropay accounts created by the FPPA can open up entire new markets for commerce. There is no disputing the fact that the internet is the ideal platform for high-volume sales of low-priced content. But the proper price point for most internet content is clearly below 20 cents per view, often less than a penny per view—far below the minimum transaction charge for credit cards.

In this regard, the internet has long needed a universal micropay solution. Indeed, it was originally designed with the expectation that a universal micropay solution would be available.[12] But all previous attempts have failed to gain critical mass because they were all one-way systems: designed to move money only from consumers to sellers. There were never enough consumers willing to gamble $20 on pre-funding a micropay account based on the promise that one day content providers would be signing up to offer content on that same micropay platform.

This problem would be solved by the FPPA. It would eliminate the need for consumers to pre-fund their micropay accounts. Everyone will have them, perhaps even multiple accounts, with Google, Facebook Twitter, and others. Or perhaps the micropay market will converge toward a single vendor or cryptocurrency. Alternatively, each major data aggregator could choose to create their own cryptocurrency in an effort to capture additional financial benefits and exchange fees. In this regard, the FPPA leaves room for innovation and market forces to shape the future of micropay systems by including the option for the required audit trails to be provided through a blockchain (an open ledger).

In any event, data aggregators would be in position to earn additional revenue though both exchange fees and the sale of their own additional services or content at micropay rates. Indeed, companies like Google that are both data aggregators and content providers would have an inside track for collecting both fees for micropay transactions and payments for content.

In addition, data aggregators will also benefit from collecting even more data on each micropay purchase. Since recent purchase behaviour is some of the most valuable data, the ability to facilitate and track micropayments will further improve targeted marketing services.

Most importantly, this micropay economy would not be limited to simply the ad dollars consumers received for use of their data. If advertisers are effective, they will sell more than they spend on advertising. As a result, if users buy more through their micropay accounts than they receive, they will need to add additional funds from traditional sources.

In other words, the micropay economy managed by data aggregators is likely to be much larger than that for advertising alone. It will also include the online content and service economy, especially for purchases under $2, which are impractical for credit and debit card transactions. Moreover, as people become comfortable using a micropay platform, even if it is based on a cryptocurrency, they will more comfortable using it for high-end purchases. Data aggregators who establish themselves as micropay leaders will therefore have an inside track on processing of purchases of any size, both online and in physical stores. This may be attractive to consumers, also, because tracking the purchases they make in every area of their lives can increase the value of their own data and how much they can earn.

Notice of law enforcement data searches

The draft of the FPPA I have offered is silent regarding notices in the audit trail regarding data that is shared with law enforcement agencies. The question of when and how data should be provided to government agencies in compliance with duly issued warrants, or under laws such as the Patriot Act which may allow broad powers of

[12] Zeynep Tufecki, "Shouldn't We All Have Seamless Micropayments By Now?", *Wired*, (21 January 2018), *https://www.wired.com/story/shouldnt-we-all-have-seamless-micropayments-by-now/* [Accessed 27 June 2019].

surveillance, is beyond the scope of this article. But it is worth noting that the audit trail required by the FPPA would provide a means to identify government requests for data in order to give proper notice to individuals and, through investigative reports, to the general public.

To provide law enforcement an opportunity to examine data without prematurely alerting suspects, it would be reasonable to require that notice of the data-sharing with law enforcement agencies would not appear in the audit trail for a specific number of days or weeks after the release of the data to government agencies. But there is a strong argument for a requirement to eventually insert a notice that data was provided to the government agency into an individual's audit trail in order to provide a mechanism for citizens to monitor the degree and scope of government investigations utilising their data.

Summary

In short, the FPPA puts an end to the idea that data collected about individuals is entirely owned by data aggregators who can do with it as they will. Specifically, the FPPA gives individuals immutable rights relative to the data that aggregators have collected about them. These include (1) the right to know when and how their data is used; (2) the right to receive (as default) at least a nominal payment of one-thousandth of a cent each time their data is used; and (3) a right to modify the payment required to use their data for future uses.

Through these provisions, the FPPA recognises that data aggregators and the people about whom they have collected data have a shared ownership interest in that data. That data has a value that can be exploited to the benefit of both parties, but the fair use of that data requires transparency in the form of audit trails and the ability of consumers to modify the terms (by way of a monetary value) for ongoing use of their data.

The rights and responsibilities attached to personal data created by the FPPA provide a pathway to eliminate suspicion and resentment against data aggregators. In addition, by priming the pump for a new micropay economy, this solution creates new opportunities and benefits for all parties: data aggregators, advertisers, content providers and individuals.