PREDICTIVE ANALYTICS, PERSONALIZED MARKETING AND PRIVACY

TOMISLAV BRACANOVIĆ

Abstract. The article examines whether predictive analytics-based personalized marketing (PABPM) violates privacy. After explaining what PABPM is and reviewing some typical concerns over its impact on privacy, three prominent theories of privacy are analyzed as possible grounds for criticizing PABPM: Warren and Brandeis's "the right to be let alone" theory, Prosser's "fourfold" or "fragmented" theory, and Westin's "control over personal information" theory. It is argued that none of them provides a solid ground against PABPM: Warren and Brandeis's theory due to its imprecision and historical distance from contemporary technologies, Prosser's theory due to its conceptual incompatibility with PABPM, and Westin's theory due to its inconsistency with a number of widely accepted social practices and ethical principles. The purpose of the article is not to argue that nothing is morally wrong with PABPM, only that its moral wrongness, if there is any, cannot be captured using the language of privacy.

Keywords: predictive analytics, personalized marketing, privacy, personal information, presumed consent.

1. INTRODUCTION

This article examines whether predictive analytics-based personalized marketing (PABPM) violates privacy. Section (2) explains what PABPM is, describes one of its applications and outlines some concerns over its impact on privacy. Sections (3), (4) and (5) analyze three theories of privacy as possible grounds for the claim that PABPM violates privacy: Warren and Brandeis's "the right to be let alone" theory, Prosser's "fourfold" or "fragmented" theory, and Westin's "control over personal information" theory. It is argued that none of them provides a solid ground against PABPM: Warren and Brandeis's theory due to its imprecision and historical distance from contemporary technologies, Prosser's theory due to its conceptual incompatibility with PABPM, and Westin's theory due to its

Tomislav Bracanović ✉
Institute of Philosophy, Zagreb
Ulica grada Vukovara 54, 10000 Zagreb, Croatia
e-mail: tomislav@ifzg.hr

Rev. Roum. Philosophie, **63,** *2*, p. 263–275, Bucureşti, 2019

inconsistency with a number of widely accepted social practices and ethical principles. The purpose of the article – as emphasized in the conclusion (6) – is not to argue that nothing is morally wrong with PABPM, only that its wrongness, if there is any, cannot be captured using the language of privacy.

2. PREDICTIVE ANALYTICS-BASED PERSONALIZED MARKETING

Predictive analytics is the practice of analyzing large amounts of data – using techniques like data mining and machine learning – with the purpose of predicting future events, including future human behavior and preferences. It is applied in areas like stock market, political campaigning, health care provision and prevention of crime and child abuse.[1] A widespread use of predictive analytics is in "personalized marketing" – a form of marketing that does not advertise products or services to the general public but creates offers "tailored to" individual customers instead. Basically, it comes down to collecting data about customers' past purchases or services used and analyzing them in order to predict their preferences for additional products or services.

The following example illustrates how PABPM works: Target, one of the major US retailers, wanted to find out which customers of theirs are pregnant and when is their due date. If they identify expectant mothers, they will be able to send them personalized ads or coupons for baby products and make extra profit. The solution came from predictive analytics specialists. They analyzed Target's baby shower registry containing voluntarily provided data like the expectant mother's name, her spouse's name and her due date. The registry was a training ground for algorithms designed to detect prospective parents' shopping patterns. It turned out that there were around 25 products (like unscented lotion, cotton balls, calcium, magnesium and zinc) indicative of their buyer's pregnancy. Profiles of individual customers were created, comprising data like purchases with Target-issued credit cards, use of frequent buyer tags at the register, coupons redeemed, surveys filled out, online purchases and similar. Target's algorithms analyzed these data and assigned each customer her "pregnancy score". On the basis of this score, personalized ads and coupons for products like cribs, feeding bottles and diapers were created and sent to individual customers.[2] This led to the following incident: "… a man walked into a Target outside Minneapolis and demanded to see the manager. He was clutching coupons that had been sent to his daughter, and he was angry… 'My daughter got this in the mail!' he said. 'She's still in high school, and you're sending her coupons for baby clothes and cribs? Are you trying to

[1] Some applications are reviewed in Eric Siegel, *Predictive analytics: The power to predict who will click, buy, lie, or die* (Hoboken, NJ: Wiley, 2013).

[2] The example is adapted from Charles Duhigg, "How Companies Learn Your Secrets", *New York Times Magazine*, February 16, 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (website visited: September 19, 2019) and Siegel, *Predictive analytics*.

encourage her to get pregnant?' The manager didn't have any idea what the man was talking about. He looked at the mailer. Sure enough, it was addressed to the man's daughter and contained advertisements for maternity clothing, nursery furniture and pictures of smiling infants. The manager apologized and then called a few days later to apologize again. On the phone, though, the father was somewhat abashed. 'I had a talk with my daughter,' he said. 'It turns out there's been some activities in my house I haven't been completely aware of. She's due in August. I owe you an apology.'"[3]

It is widely believed that PABPM is a threat to privacy. Solove claims that "our privacy is under assault" because "businesses are collecting an unprecedented amount of personal data, recording the items we buy at the supermarket, the books we buy online, our web-surfing activity, our financial transactions, the movies we watch, the videos we rent, and much more."[4] Spencer suggests that merchants "cannot overlook the privacy concerns that predictive analytics can raise", because "[c]onsumers may be uncomfortable allowing secret algorithms to determine their prices, service, and eligibility based on other consumers' past behaviors."[5] Richards draws attention to "the increased persuasive power that data-based analytics give to already powerful entities – advertisers, corporations, political machines, and government entities", warning us that "the degree to which these developments are a problem is impossible if we think about privacy or information rules as only hiding discrete pieces of discreditable information about ourselves."[6] The same concerns permeate many media articles about PABPM and similar practices.

The language of privacy seems like the natural framework for formulating moral and legal concerns over PABPM. The problem that emerges, however, is that concepts like "privacy" and the "right to privacy" are vague and open to different interpretations. As Thomson remarked: "Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is."[7] Therefore, if we wish to criticize PABPM as a threat to privacy, we need to spell out what we mean by "privacy" or which theory of privacy we subscribe to.

In what follows, three theories of privacy – Warren and Brandeis's, Prosser's and Westin's – will be examined. All of them are the *loci classici* of philosophical and legal debates on privacy and they often constitute (at least partially) the building blocks of contemporary approaches to privacy issues raised by new technologies. Moreover, all three theories, when viewed together, are conceptually

[3] Duhigg, "How Companies Learn Your Secrets".

[4] Daniel J. Solove, "The Meaning and Value of Privacy", in *Social dimensions of privacy: Interdisciplinary perspectives*, ed. Beate Roessler and Dorota Mokrosinska (Cambridge: Cambridge University Press, 2015), p. 71.

[5] Shaun B. Spencer, "Predictive Analytics, Consumer Privacy, and Ecommerce Regulation", in *Research handbook on electronic commerce law*, ed. John A. Rothchild (Cheltenham, Northampton: Edward Elgar Publishing, 2016), p. 517.

[6] Neil M. Richards, "Four Privacy Myths", in *A world without privacy: What law can and should do?*, ed. Austin Sarat (Cambridge: Cambridge University Press, 2015), p. 69.

[7] Judith Jarvis Thomson, "The Right to Privacy", *Philosophy & Public Affairs* 4, no. 4 (1975): 295.

very diverse (even mutually opposed) and as such hold the promise of providing a theoretical foundation for the commonsense belief that PABPM threatens our privacy. It will be argued, however, that none of them poses a serious threat to PABPM.

3. PRIVACY AS "THE RIGHT TO BE LET ALONE"

The right to privacy is often described as "the right to be let alone". The phrase became widespread thanks to Warren and Brandeis. They argued that the common-law allows for establishing the right to privacy, as the right independent of other rights like the right to liberty or the right to property. As they claimed, "the existing law affords a principle which can properly be invoked to protect the privacy of the individual"[8] and the right to privacy should be of the same weight as "the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed."[9]

The motive behind Warren and Brandeis's plea for the right to privacy was an unease with "inventions and business methods" of their time. Specifically: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'."[10] In order to protect the "bounds of propriety and decency", they proposed the introduction of the separate right to privacy as the "right to be let alone". This right should rest on something they call the principle of "inviolate personality". Although they omit to explain the exact nature of this principle, it seems closely related to a family of notions like dignity, individuality and integrity. Bloustein reads Warren and Brandeis's proposal as suggesting that "[t]he man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity."[11] According to Schoeman, Warren and Brandeis wanted to emphasize that privacy interest is "connected in a profound way with the recognition of human moral character" and to "underscore that the law recognizes the moral and spiritual integrity of individuals, as well as their material interests."[12]

[8] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review* 4, no. 5 (1890): 197.

[9] Ibid., p. 205.

[10] Ibid., p. 195.

[11] Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", in *Philosophical dimensions of privacy: An anthology*, ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984), p. 188.

[12] Ferdinand David Schoeman, "Privacy: Philosophical Dimensions in the Literature", in *Philosophical dimensions of privacy: An anthology*, ed. Ferdinand David Schoeman (Cambridge: Cambridge University Press, 1984), p. 15.

Is it possible, relying on Warren and Brandeis's "the right to be let alone", to criticize PABPM as a threat to privacy? The answer to this question should be negative, for two reasons. The first reason is its lack of precision, reflected in the fact that Warren and Brandeis "never define what privacy is"[13] and the fact that their "[u]nderstanding privacy as being let alone does not inform us about the matters in which we should be let alone."[14] This makes it difficult to see how PABPM could jeopardize "inviolate personality" as the core principle of the theory, or any of its associated values like "dignity", "individuality" or "moral and spiritual integrity". One could claim, actually, that PABPM allows people to be "let alone" even more than they would have been without it. For example, people are no longer exposed to numerous ads from all sorts of businesses, not to mention the intrusive telephone or door-to-door sales; thanks to PABPM, they are exposed only to ads they are likely to be interested in. It would be difficult to show that their personalities were violated in some unique way in which personalities of people exposed to traditional advertising were not. If "being let alone" is what privacy is about, predictive analytics could actually be a privacy-enhancing technology.

The second reason is its historical distance from contemporary technologies. Privacy concerns over early 21st century technologies are different from privacy concerns over late 19th century technologies. Warren and Brandeis's principal examples of privacy threatening technologies – the portable camera ("instantaneous photographs") and the printing press – have little in common with PABPM and technologies like data mining or machine learning. "Social ontology" is also different. As Taylor, Floridi and van der Sloot suggest, most data processing technologies today are "transcending the individual", because "data is no longer gathered about one specific individual or a small group of people, but rather about large and undefined groups", and this "challenges the very foundations of most current existing legal, ethical and social practices and theories."[15] Therefore, even if Warren and Brandeis's theory was adequate for imposing legal or moral limits to technologies of their society and time, it does not follow that it is adequate for imposing similar limits to technologies of our society and time.

It is also possible to read Warren and Brandeis's article contrary to their intentions, i.e. as supporting the view that "privacy" is not an objective value, but a historically relative notion that changes as technologies change. According to a report by Castro and McQuinn, many new technologies have "privacy panic cycles" consisting of several stages: "It is the cycle of panic that occurs when privacy advocates make outsized claims about the privacy risks associated with

[13] Ibid., p. 14.

[14] Daniel J. Solove, *Understanding privacy* (Cambridge, Mass., London: Harvard University Press, 2008), pp. 17–18.

[15] Linnet Taylor, Luciano Floridi and Bart van der Sloot, "Introduction: A New Perspective on Privacy", in *Group privacy: New challenges of data technologies*, ed. Linnet Taylor, Luciano Floridi and Bart van der Sloot (Cham: Springer, 2017), p. 5.

new technologies. Those claims then filter through the news media to policymakers and the public, causing frenzies of consternation before cooler heads prevail, people come to understand and appreciate innovative new products and services, and everyone moves on."[16]

It is interesting that portable camera – for Warren and Brandeis the ultimate threat to privacy – is for Castro and McQuinn the paradigmatic example of technology going through "privacy panic cycle". According to their report, portable camera was met with hostility after its introduction in 1888: warnings were published against those carrying them, they were sometimes prohibited in public spaces, vigilance groups protected women from camera-carrying intruders, even president Roosevelt is reported telling a boy who tried to take a picture of him: "You ought to be ashamed of yourself." However, privacy panic over portable camera was over by 1910. According to Castro and McQuinn, privacy panic over PABPM ("behavioral advertising") currently is at its peak, but it is not unreasonable to expect it to deflate within a foreseeable time just as it was the case with portable camera. The historical lesson here is that privacy concerns over PABPM may be a matter of social adjustment to new technologies, not a matter of violation of some objective value or right.

4. THE "FOURFOLD" OR "FRAGMENTED" THEORY OF PRIVACY

If Warren and Brandeis's theory is an unstable ground for criticizing PABPM, it is logical to turn to its influential alternative: the theory proposed in 1960 by Prosser. Whereas Warren and Brandeis were "privacy realists" and saw privacy as specific interest and right irreducible to any other interest or right, Prosser was a "privacy reductionist" and saw privacy as a second-order right or interest, reducible to more fundamental rights and interests like those related to property, reputation and emotional tranquility. Prosser intention was not to suggest that privacy needs no protection, but to highlight its "complex" or "composite" nature. He believed that any violation of what Warren and Brandeis believed is the distinctive "right to be let alone" reduces to one – or some combination – of the following four violations:

(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
(2) Public disclosure of embarrassing private facts about the plaintiff.
(3) Publicity which places the plaintiff in a false light in the public eye.
(4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[17]

[16] Daniel Castro and Alan McQuinn, *The privacy panic cycle: A guide to public fears about new technologies* (Washington, DC: The Information Technology & Innovation Foundation, 2015), p. 1. Available at: http://www2.itif.org/2015-privacy-panic.pdf

[17] William L. Prosser, "Privacy", *California Law Review* 48, no. 3 (1960): 389.

Prosser's theory, sometimes referred to as the "fourfold"[18] or "fragmented"[19] theory, provides a solid ground for classifying a range of actions as privacy violations. It also corresponds well with what many people consider a privacy violation, e.g. peeping into someone's bedroom (intrusion), publishing someone's explicit photos (embarrassment), spreading gossip about someone (false light in the public eye) or using someone's picture or name to advertise a product or service (appropriation). However, despite the fact that many people perceive PABPM as an obvious threat to privacy, it is interesting to see how resistant it is to criticisms based on Prosser's fragments. Fragment (4) – appropriation of someone's name or likeness in order to make profit – is inapplicable (PABPM is about profit, but it involves no appropriation of anyone's name or likeness). The same can be said of fragment (2) – public disclosure of embarrassing private facts – and (3) – placing someone in a false light in the public eye. As it does not disclose anyone's private facts to the public or to any third party, PABPM gets a clean bill of health with respect to these two fragments as well.

A possible reply is that, when it comes to Target's "pregnancy score" coupons, someone's private facts were disclosed: a teenager's pregnancy to her father. It may be far-fetched, however, to qualify this as "disclosure", for two reasons: Firstly, the coupons contained no information about particular persons. Secondly, the father had no idea that the coupons were the end product of PABPM and could not infer from their content, therefore, that his daughter is pregnant. The coupons only accidentally led to his discovery, which can be illustrated by the following scenario: Imagine that Target did not use "personalized marketing" (tailoring ads to *individuals*), but "market segmentation" (tailoring ads to *groups* of individuals) instead. As a result, the same coupons were sent to all female customers aged between 16 and 40 years. Everything else being equal, this would trigger the same reaction of this father (and subsequent discovery of pregnancy) but it would be equally accidental. There was nothing inherent to this case of PABPM, therefore, that can be qualified as disclosure of someone's private facts.

What remains to be seen is how PABPM fares with respect to fragment (1) – the intrusion upon someone's seclusion or solitude, or into his or her private affairs. The meaning of this fragment is vague because it refers to vague notions like "seclusion", "solitude" and "private affairs". According to a standard interpretation, however, it comes down to "the physical intrusion into the plaintiff's premises and eavesdropping (including electronic and photographic surveillance, bugging, and telephone-tapping)", which must satisfy three requirements: "(a) there must be an actual prying; (b) the intrusion must offend a reasonable man; (c) it must be an intrusion into something private."[20]

[18] Raymond Wacks, *Privacy: A very short introduction* (Oxford: Oxford University Press, 2010).

[19] Lior Jacob Strahilevitz, "Reunifying Privacy Law", *California Law Review* 98, no. 6 (2010).

[20] Wacks, *Privacy*, p. 57.

PABPM involves no "physical intrusion" or "eavesdropping". It is possible, as we have seen, that it even helps us to be "let alone" and free from intrusions. It is also possible that PABPM is no threat to privacy because it involves no human perpetrator. In PABPM human is "out of the loop" as most of its steps – collecting data about customers' past purchases, calculating which products they might like and creating personalized ads – are performed by machines. In other words, there is no privacy violation because there is no human violator. Of course, this does not apply to all uses of predictive analytics or data mining. For example, Müller argued that a similar use of machines for surveillance purposes would be a privacy violation because data analysis would have to be finalized by a human.[21] However, as long as PABPM is automatized to the extent that no human makes decisions about particular customers, its impact on privacy is non-existent. It is as inoffensive, to use Müller's example, as "a computer at the phone company that processes call minutes and prints a bill at the end of the month."[22]

People at Target were aware that PABPM creates the impression with their customers that "someone" is spying on them. One executive was quite open about this: "With the pregnancy products, though, we learned that some women react badly… Then we started mixing in all these ads for things we knew pregnant women would never buy, so the baby ads looked random. We'd put an ad for a lawn mower next to diapers. We'd put a coupon for wineglasses next to infant clothes. That way, it looked like all the products were chosen by chance."[23] The impression that PABPM involves something "intrusive" and "offensive" related to privacy is obviously hard to avoid. The next section examines whether this impression can be justified with the "control over personal information" theory of privacy.

5. PRIVACY AS "CONTROL OVER PERSONAL INFORMATION"

"Control over personal information" theory was formulated in 1967 by Westin as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[24] According to Westin's more recent definition, privacy is "the claim of an individual to determine what information about himself or herself should be known to others", which involves "when such information will be obtained and what uses will be made of it by others."[25] The theory found its influential expression in the

[21] Vincent C. Müller, "Would You Mind Being Watched by Machines? Privacy Concerns in Data Mining", *AI & Society* 23, no. 4 (2009): 530.

[22] Ibid.

[23] Duhigg, "How Companies Learn Your Secrets".

[24] Alan Westin, *Privacy and freedom* (New York: Atheneum, 1967), p. 7.

[25] Alan Westin, "Social and Political Dimensions of Privacy", *Journal of Social Issues* 59, no. 2 (2003): 431.

European Union's *General Data Protection Regulation* that states that "[t]he protection of natural persons in relation to the processing of personal data is a fundamental right" and that "[n]atural persons should have control of their own personal data."[26]

"Control over personal information" theory is a challenge to PABPM. It derives its force from the combination of two concepts: *personal information* (in the sense of information that uniquely identifies a person) and *control* (in the sense that such information is not to be used, for whatever purposes, without permission of the person concerned). Accordingly, even if it involves nothing like eavesdropping, physical intrusion, appropriation or public disclosure of private facts, an act that deprives an individual of control over his or her personal information is a privacy violation. Returning to Target's PABPM: "One can assume that the daughter in Target's pregnancy prediction score did not want Target to know that she was pregnant. After all, she apparently did not sign up for Target's baby shower registry. If Target had asked her in a survey whether she was pregnant, she likely would have said no. But when she shared all of her shopping habits with Target, she could not possibly know that she was also sharing secondary evidence that Target would use to generate a pregnancy prediction score. Had the daughter known what Target could learn from her purchases, she might have exercised control over what Target could learn about her by paying in cash or shopping elsewhere. But that was not an option."[27]

It may be true that the daughter did not want Target to know that she was pregnant and would have answered no if asked whether she was. Nevertheless, it does not necessarily follow that this application of PABPM was a privacy violation. The crucial problem with the "control over personal information" theory of privacy, as it should become clear, is the fact that rejection of PABPM on its basis would be inconsistent with a number of widely accepted social practices and ethical principles.

The initial argument in defense of PABPM against the "control over personal information" theory draws on the fact that the information it typically collects is already publicly available and out of individual's control or the individual has no interest to control it in the first place. The point is this: although a retail company can extract a lot of information about people on the basis of products they buy, the same information could be extracted from their publicly visible behavior and appearance, like their clothes, cars, tattoos, sports or social events attended, food deliveries, garbage in front of their houses (the list could be continued). As part and parcel of our social life, details like these are usually out of our control, but they do allow, without any intrusion, creation of our individual profiles comparable to those created by PABPM. "Control over personal information" theory of privacy

[26] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", *Official Journal of the European Union* L119 (2016): 1–2.

[27] Spencer, "Predictive Analytics, Consumer Privacy, and Ecommerce Regulation", p. 500.

has a problem with consistent application across various areas of life because of its potential to make "most interpersonal contact in society a privacy invasion."[28]

In his criticism of predictive analytics, Sprague acknowledges that "[t]he principal privacy conundrum posed by predictive analytics is that data mining relies to a large extent on 'public' information – it derives from transactions and social interactions that are often generally observable."[29] It is equally important in this context that people are far from reluctant to renounce control over their personal information by filling out all kinds of survey forms, either for free or for a cheap price (e.g. in exchange for gifts or discounts). In other words, people do not see a large portion of their "personal information" as an intrinsic value (comparable to life, health or liberty) that needs to be protected at all cost. What follows is that PABPM violates no interest in privacy because – given the nature of information it collects and the way people generally perceive such information – there is no reason to believe that this interest exists or that it has the strength sufficient to justify claims about privacy violation. In other words, their consent to collect such information can be reasonably presumed. The situation is analogous to the one hypothesized by Thomson: "Suppose that my husband and I are having a fight, shouting at each other as loud as we can; and suppose that we have not thought to close the windows, so that we can easily be heard from the street outside. It seems to me that anyone who stops to listen violates no right of ours; stopping to listen is at worst bad, Not Nice, not done by the best people. But now suppose, by contrast, that we are having a quiet fight, behind closed windows, and cannot be heard by the normal person who passes by; and suppose that someone across the street trains an amplifier on our house, by means of which he can hear what we say; and suppose that he does this in order to hear what we say. It seems to me that anyone who does this does violate a right of ours, the right to privacy..."[30]

Just as Thomson's couple has no ground to complain about the passer-by collecting their personal information, retail store customers have no ground to complain about their personal information being collected for PABPM purposes. Their consent is reasonably presumed as long as the information collected is of the same nature as the information they leave open to the public eye. It is irrelevant, to use the metaphor by Abelson, Ledeen and Lewis,[31] whether control over our personal information was taken over by one "Big Brother" like Target or by many "Little Brothers" like our neighbors or passers-by.

The above argument in defense of PABPM can be additionally supported by three ethical principles: "ends-means" principle, principle of consistency and "ought implies can" principle. Consider first the "ends-means" principle that says,

[28] Solove, *Understanding privacy*, p. 25.

[29] Robert Sprague, "Welcome to the Machine: Privacy and Workplace Implications of Predictive Analytics", *Richmond Journal of Law & Technology* 21, no. 4 (2015): 4.

[30] Thomson, "The Right to Privacy", p. 296.

[31] Hal Abelson, Ken Ledeen and Harry Lewis, *Blown to bits: Your life, liberty, and happiness after digital explosion* (Upper Saddle River, NJ: Addison-Wesley, 2008).

in Kant's wording, that "all rational beings stand under the *law* that each of them is to treat himself and all others *never merely as means* but always *at the same time as ends in themselves*."[32] The principle is explained by O'Neill: "To use someone as a *mere means* is to involve them in a scheme of action *to which they could not in principle consent*. Kant does not say that there is anything wrong about using someone as a means. Evidently we have to do so in any cooperative scheme of action. If I cash a check I use the teller as a means, without whom I could not lay my hands on the cash; the teller in turn uses me as a means to earn his or her living. But in this case, each party consents to her or his part in the transaction. Kant would say that though they use one another as means, they do not use one another as *mere* means."[33]

Although it involves collection of personal information without its owner's explicit consent, PABPM does not look as "a scheme of action to which people could not in principle consent", for at least two reasons. One reason is that most people, as already mentioned, evidently have no interest to hide the same information in relevantly similar situations. Moreover, the fact that people often do consent to similar "schemes of action" implies that they are not likely to consider the use of their personal information for PABPM as morally outrageous. The second reason is the fact that PABPM is a scheme of action designed to benefit those whose information is collected. According to Abelson, Ledeen and Lewis: "The most obvious reason not to worry about giving information to a company is that you do business with them, and it is in your interest to see that they do their business with you better. You have no interest in whether they make more money from you, but you do have a strong interest in making it easier and faster for you to shop with them, and in cutting down the amount of stuff they may try to sell you that you would have no interest in buying. So your interests and theirs are, to a degree, aligned, not in opposition."[34]

The above reading of the "ends-means" argument might not apply in circumstances when someone has no choice but to shop with a particular retailer. However, as long as one can choose with whom to do business, probably the worst thing about PABPM is not its moral wrongness but its lack of business etiquette. This problem usually solves itself thanks to the "invisible hand" of free market, in the sense that "businesses are unlikely to surreptitiously gather or use the personal information about their customers in invasive ways if doing so would alienate their consumers and hurt their business."[35] In Thomson's words, PABPM may be done in a way that is "not nice", but it does not violate privacy.

The second ethical principle supporting our "presumed consent" argument for PABPM is consistency. The principle, to use Hare's formulation, forbids us to

[32] Immanuel Kant, *Groundwork of the Metaphysics of Morals* (Cambridge: Cambridge University Press, 1998), p. 41.

[33] Onora O'Neill, "A Simplified Account of Kant's Ethics", in *Contemporary moral problems*, ed. James E. White (St. Paul: West Publishing Company, 1994), p. 44.

[34] Abelson, Ledeen and Lewis, *Blown to bits*, p. 39.

[35] Castro and McQuinn, *The privacy panic cycle*, p. 28.

"make different moral judgments about actions which we admit to be exactly or relevantly similar."[36] Consider the following scenario: Peter runs a fruit stand. One day he tells John: "Your wife was here this morning, but she appears to have forgotten to buy oranges as usual. Would you like to buy them now? Actually, let me offer you this basket of oranges, lemons and grapefruits for the same price. I am sure your wife would love that."

Did Peter violate John's privacy? Let us assume he did not (on the contrary, John is grateful and will continue shopping at Peter's because it saves him time and money). What needs to be noted then is the similarity between Peter's behavior and PABPM. They both involve the same four components: (1) a desire to increase profit by pleasing customers, (2) remembering customers' past purchases, (3) estimating what customers might like in the future, and (4) making offers to customers for products or discounts. Given there is no relevant difference between them, consistency dictates that either both of them are to be blamed for violating privacy or that neither of them is to be blamed. Therefore, if we believe Peter did nothing wrong, then we should believe Target did nothing wrong either.

If we assume that Peter violated John's privacy, we would have to conclude that Target violated its customers' privacy too. The principle of consistency would be preserved just as it was in the previous scenario. However, the problem would arise with the third ethical principle: "ought implies can" principle that claims that no one has the moral duty do to something he or she is unable to do. If we claim that Peter violated John's privacy, we would have to explain which component of his behavior was decisive for this violation. Components (1), (3) and (4) have to be excluded because they are essential ingredients of every business enterprise. What remains is component (2): remembering customers' past purchases. "Control over personal information" theory would imply that both Peter and Target have a duty not to remember information they intentionally or unintentionally collect about their customers' preferences. This kind of mental (and economic) self-handicapping is surely not something any merchant can do. Therefore, neither Peter nor Target can be obliged to do this, and Target's predictive analytics-based personalized marketing is as innocuous as Peter's common sense-based personalized marketing.

6. CONCLUSION

The purpose of this article was to articulate a defense of PABPM against the charges based on three theories of privacy: Warren and Brandeis's "the right to be let alone" theory, Prosser's "fourfold" or "fragmented" theory and Westin's "control over personal information" theory. This defense can be summarized as follows: PABPM does not violate privacy because (a) it discloses no personal information to the public or to any third party; (b) it involves no physical intrusion,

[36] Richard M. Hare, *Freedom and reason* (Oxford: Clarendon Press, 1963), p. 33.

prying or eavesdropping; (c) no appropriation of anyone's name or likeness takes place; (d) all personal information is acquired with explicit consent or with reasonable assumption of consent, (e) it benefits individual customers; (f) it helps people to "be let alone" and preserve their privacy; and (g) it is consistent with a number of widely accepted social practices and ethical principles.

The basic claim of the article is not that there is nothing morally problematic with PABPM. It could collide with various moral values. For example, personal information may be processed or stored in a way that creates safety risks to individuals. Questions of equality or justice may arise in cases when algorithms deployed generate different offers for different individuals on the basis of characteristics like ethnicity or race. An individual autonomy may be threatened as companies gain more power to predict people's preferences and nudge them to behave in ways that may not be in their best interest. PABPM obviously raises a number of diverse ethical issues not necessarily related to privacy. An overemphasis on privacy, therefore, might lead us astray from the more pressing problems pertaining to PABPM, especially if the language of privacy, as it was argued in this article, is not the best tool for capturing its potential moral wrongness.

Acknowledgments: Earlier versions of this article were presented at the conference *Contemporary Philosophical Issues* (Rijeka, April 2018), the regular colloquium of the Institute of Philosophy (Zagreb, May 2018), and the conference *Ethical Issues: Theoretical & Applied* (Bled, June 2018). I am grateful to all three audiences for constructive comments. The article was completed as part of the research project *Ethics and Everyday Life*, conducted since 2019 at the Institute of Philosophy, Zagreb.