Editors: Angela Sasse, a.sasse@cs.ucl.ac.uk | Alessandro Acquisti, acquisti@andrew.cmu.edu

Informed Consent:
We Can Do Better to Defend Privacy

Frederik Zuiderveen Borgesius | University of Amsterdam

Currently, policymakers focus heavily on the idea of informed consent as a means to defend privacy. In many countries, companies are required by law to obtain individuals' consent before using their data for certain goals, an approach that aims to empower people to make privacy choices that are in their best interest. But behavioral studies cast doubt on this approach's effectiveness, as people tend to agree with almost any request they see on their screens. A combined technique that both protects and empowers individuals would improve privacy.

Behavioral Targeting and Privacy

Behavioral targeting is a marketing technique where people's online behavior is tracked and the collected information is used to display individually targeted Web advertisements to people.[1] The captured information encompasses many online activities: the articles people read, the videos they watch, the terms they search for, and so on. Individual profiles can be enriched with mobile device users' up-to-date location data and other data gathered on- and offline. Some email or social network providers analyze the content of private messages for marketing purposes. Vast amounts of information about hundreds of millions of people are collected for behavioral targeting.

In principle, behavioral targeting can benefit both companies and consumers. Thanks to advertising, people can enjoy access to online translation tools, news sites, email and social networking, videos, music, and other forms of entertainment without explicitly paying with money. However, advertising doesn't always require monitoring people's behavior. For instance, ads for cars could be displayed on websites about cars. As such, it's unclear whether behavioral targeting is needed to fund "free" websites and services.

Behavioral targeting raises three main privacy concerns: *chilling effects*, a lack of control over personal information, and the risk of unfair discrimination and manipulation. As with other types of surveillance, people might adapt their behavior if they suspect their activities are being monitored. This is called a chilling effect. In addition, individuals don't have control over data collected about them. They don't know which information is collected, how it's being used, or with whom it's shared. Large-scale personal data storage also brings risks: a data breach could occur, leading to data being used for identity fraud.

Behavioral targeting also enables social sorting and discriminatory practices. Companies can classify people as "targets" or "waste" and treat them accordingly.[1] For instance, an advertiser could use discounts to lure affluent people

1540-7993/15/$31.00 © 2015 IEEE Copublished by the IEEE Computer and Reliability Societies March/April 2015

to become regular customers but exclude less affluent people from the campaign. Some fear that behavioral targeting could be used to manipulate people: personalized advertising could become so effective that advertisers gain an unfair advantage over consumers. Others worry that excessive personalization can lead to a *filter bubble:* if algorithms select the information we see on the Web, each us of might see a different image of the world.[2] Simply stated, personalized advertising and other content could surreptitiously steer people's thoughts and actions. This fear seems most relevant when companies personalize not only ads but other content and services.

Informed Consent in Data Privacy Law

Informed consent and individual choice play a central role in many data privacy rules around the world. For instance, the Organisation for Economic Co-operation and Development's (OECD's) privacy guidelines state that personal data should be obtained "where appropriate, with the knowledge or consent of the data subject."[3] In the US, the proposed Privacy Bill of Rights emphasizes the importance of individual choice regarding the use of data.[4] Numerous Federal Trade Commission (FTC) cases regarding this issue signal that the FTC thinks that prominent notice and opt-in consent are necessary to collect sensitive personal information.[5]

The EU's e-Privacy Directive is another example of informed consent's active role in data privacy law.[6] This directive requires any party that stores or accesses information on a user's device to obtain the user's informed consent. This applies to many tracking technologies, including cookies. Valid consent requires a freely given, specific, and informed indication of an individual's wishes. People can express their will in any form, but mere silence or inactivity isn't an expression of will. Some companies suggest they can presume implied consent if people don't block tracking cookies in their Web browser,[7] but this interpretation of the law seems incorrect. EU data protection authorities say that a user who left her browser settings untouched didn't consent to being tracked.[8]

In addition, EU law requires consent to be freely given: consent under too much pressure isn't valid. Nevertheless, in most circumstances, current data privacy law will probably allow companies to offer take-it-or-leave-it choices. For example, website publishers are not prohibited from installing tracking walls that deny entry to visitors that don't consent to being tracked for behavioral targeting. But such a wall could make consent involuntary if an individual must use a website. According to the Dutch data protection authority, the national public broadcasting organization isn't allowed to use a tracking wall because the only way to access certain information online is through the broadcaster's website.[9] EU data protection authorities state that consent should be given freely, but they don't say that current law prohibits tracking walls in all circumstances.[10]

Informed Consent in Practice

Economic theory can help us analyze practical problems with consent to behavioral targeting. From an economic perspective, consenting to behavioral targeting can be seen as entering a market transaction with a company. But this transaction is plagued by information asymmetries. Research shows that many people don't know to what extent their behavior is tracked.[11] Therefore, their "choice" to disclose data in exchange for using a service can't be informed. Furthermore, tracking information is collected, combined, and analyzed on a massive scale. A user might only provide small bits of data, but companies could still construct detailed profiles by combining data from different sources.

But, as behavioral economics research has highlighted, even if companies sought consent for behavioral targeting, information asymmetry would remain a problem.[12] People rarely know what a company does with their personal data, and it's difficult to predict the consequences of future data usage. Companies have few incentives to offer privacy-friendly services because people can't easily assess whether a service is actually private. For instance, it's difficult for users to detect whether they're being tracked during a website visit. Indeed, it seems websites don't use privacy as a competitive advantage: people are tracked for behavioral targeting on virtually every popular website.[13] There seems to be a comparable situation for smartphone apps.

When animated by privacy control rationales, data privacy law aims to reduce the information asymmetry. For example, EU law requires companies to disclose certain information to individuals, such as the purposes for using personal data. Website publishers can use a privacy policy to comply with data protection law's transparency requirements.

However, the information asymmetry problem is difficult to solve due to transaction costs and the varying meanings of privacy policies. Reading privacy policies would cost too much time, as they're often long, difficult to understand, and vague. As a White House report puts it, "only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent."[14] In practice, data privacy law doesn't solve the information asymmetry problem.

An example is when a UK store obtained the souls of 7,500 people.[15] According to the website's terms and conditions, customers granted "a nontransferable option to claim, for now and forever more, your immortal soul," unless they opted out. By opting out, customers could save their soul and receive a £5 voucher. But few people opted out. The store later said it wouldn't exercise its rights.

Behavioral economics aims to improve the predictive power of economic theory by including insights from psychology and behavioral studies. Behavioral economics suggests that people act differently than economic rational choice theory predicts. Due to bounded rationality, people often rely on rules of thumb or heuristics. Usually these mental shortcuts work fine, but they can also lead to behavior that isn't in people's self-interest. Several biases influence privacy choices, such as the *status quo bias*—the tendency to stick with default options—and the *present bias*—the tendency to choose immediate gratification and disregard future costs or disadvantages.

An example of the status quo bias is that people are less likely to consent under an opt-in regime that requires an affirmative action for valid consent than under an opt-out regime in which people are assumed to consent if they don't object.[16] In this light, the continuous opt-in/opt-out discussion about behavioral targeting and other types of direct marketing actually concerns the question: Who benefits from the status quo bias—companies or individuals?

Many people find it hard to stick with a diet or save money due to the immediate gratification of eating or spending what they want. This is an example of the present bias. Likewise, if a website has a tracking wall and users can visit the site only if they agree to behavioral targeting, they're likely to consent, ignoring the risk of future privacy infringements.

Behavioral economics shows that using informed consent to protect privacy is fraught with problems. As mentioned, most people don't read privacy policies, and if they did, they most likely wouldn't fully understand them. Even if they did fully understand them, they likely wouldn't act. In addition, if a company's competitors exploit information asymmetry and people's biases, that company would have to do the same to stay in business. This suggests that more regulatory intervention is needed to protect privacy in the area of behavioral targeting.

It seems websites don't use privacy as a competitive advantage: people are tracked for behavioral targeting on virtually every popular website.

Individual Protection

Some data privacy laws contain rules that could defend privacy interests, even after consenting to tracking. For instance, the OECD privacy guidelines state that personal data should be protected by reasonable security safeguards.[3] Regulators in the EU and US also emphasize the need for companies to secure the data they hold.

EU data privacy law is stricter regarding "special categories" of personal data, such as data revealing race, political opinions, health status, or sexual preference. In many EU countries, using these special categories for direct marketing is prohibited; in other countries, it's allowed only with individuals' explicit consent. There are exceptions, but these aren't relevant for behavioral targeting. Some companies target advertising to individuals with arthritis or cardiovascular health issues or to disabled or handicapped consumers, meaning that they process special categories of data. Strictly enforcing the existing rules on these special categories could reduce privacy problems such as chilling effects. The rules on these special categories could be interpreted in such a way that the collection context is taken into account. For example, tracking a user's visits to websites with medical information should arguably be seen as processing special categories of data, as the company could infer health-related data from such tracking information.

Because the privacy risks involved in using health data for behavioral targeting seem to outweigh the possible societal benefits from allowing such practices, policymakers should consider prohibiting the use of any health-related data for behavioral targeting, regardless of whether the individual gives explicit consent. A question that warrants more discussion is what the scope of such restrictions should be. For example, should a prohibition of using health data for behavioral targeting include a user's visits to a website with gluten-free recipes?

Although strict enforcement of data privacy law's more protective principles could somewhat mitigate privacy problems, additional rules are likely needed. Even if opt-in systems are required, informed consent requirements won't be effective privacy protection as long as companies are allowed to offer take-it-or-leave-it choices.

Broadening the Debate

It's time to extend the privacy debate beyond informed consent.

Aiming for transparency and consent won't ensure a reasonable level of privacy. Consumer law illustrates how empowerment and protection rules can be used as complementary tools. In many circumstances, consumer law requires companies to disclose certain information, such as nutritional information and shipping costs. These transparency requirements aim to empower consumers to make decisions according to their preferences. Other rules in consumer law aim to protect consumers. For instance, some ingredients may not be used in certain foods, and many products have minimum safety standards.

It has been suggested that policymakers should focus more on data use and less on informed consent for data collection.[17] However, focusing mostly on data use has considerable risks. I argue strongly against leaving data collection mostly unregulated. Many privacy problems, such as chilling effects, already occur because of data collection. In Europe, leaving data collection unregulated would be difficult to reconcile with fundamental rights case law and treaties.[18]

So what should policymakers do about take-it-or-leave-it choices such as tracking walls? The law could prohibit tracking walls in certain circumstances. For instance, public service broadcasters often receive public funding and play a special role in educating and informing the public, and in promoting the values of democratic societies. But if people fear their behavior is being monitored, they might forgo using public service media. In this case, policymakers should prohibit public service broadcasters from installing tracking walls on their websites.

More generally, it's questionable whether it's appropriate for public sector websites to allow third-party tracking for behavioral targeting, even when people consent. In practice, public sector websites might use third-party widgets such as buttons that let visitors share content from a website to their social media accounts. Website publishers might not realize that these third-party widgets could expose visitors to privacy-invasive tracking. But because it's not evident why the public sector should facilitate tracking people's behavior for commercial purposes, policymakers should consider prohibiting all tracking for behavioral targeting on public sector websites.

Policymakers can add prohibitions to their toolbox to regulate behavioral targeting, though it would be difficult to define prohibitions so that they're not over- or underinclusive. Difficult questions lie ahead for policymakers, who must strike a careful balance between undue paternalism and protecting people. The legal protection of privacy will remain a learning process. If new rules are adopted, their practical effects will have to be evaluated. The problems with the current informed consent requirements demonstrate that regulation that looks good on paper might not effectively protect privacy in practice.

Defending Privacy with Technology

The distinction between empowerment and protection could also inform discussions about technical privacy defense tools. For example, technology could help foster meaningful transparency regarding data processing and profiling, and user-friendly mechanisms are needed to give, withhold, or retract consent. However, in some circumstances, people might benefit more from protection against risks than from being confronted with transparency and choices. Examples of more protective technical approaches include services that automatically secure personal information, metadata, or communications, regardless of the user's initiative.

There's no silver bullet to improve privacy protection in behavioral targeting. Whereas current regulations often emphasize individual empowerment without much reflection on practical issues, a combined approach could be used to both protect and empower people. To improve privacy protection, current data privacy law should be enforced more strictly, but the limited potential of informed consent as a privacy protection measure must also be taken into account. ■

References

1. J. Turow, *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*, Yale Univ. Press, 2013.
2. E. Pariser, *The Filter Bubble*, Penguin Viking, 2011.
3. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Co-operation and Development, 2013; http://oe.cd/privacy.
4. "Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," White House, Feb. 2012; www.whitehouse.gov/sites/default/files/privacy-final.pdf.
5. "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Federal Trade Commission, Mar. 2012; www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
6. "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector," European Parliament, 12 July 2002; http://eur-lex.europa.eu/LexUri

Serv/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML.
7. "Department for Business, Innovation & Skills Consultation on Implementing the Revised EU Electronic Communications Framework," Interactive Advertising Bureau, Dec. 2012; www.iabuk.net/sites/default/files/IABUKresponsetoBISconsultationonimplementingtherevisedEUElectronicCommunicationsFramework_7427_0.pdf.
8. "Opinion 2/2010 on Online Behavioural Advertising," Article 29 Data Protection Working Party, 00909/10/EN WP 171, June 2010; http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
9. Dutch Data Protection Authority, "Letter to the State Secretary of Education, Culture, and Science," 31 Jan. 2013; https://cbpweb.nl/nl/nieuws/reactie-cbp-op-gebruik-cookies-door-nederlandse-publieke-omroep.
10. "Working Document 02/2013 Providing Guidance on Obtaining Consent for Cookies," Article 29 Data Protection Working Party, 1676/13/EN WP 208, Oct. 2013; http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
11. B. Ur et al., "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising," *Proc. 8th Symp. Usable Privacy and Security* (SOUPS 12), 2012, article 4.
12. A. Acquisti and J. Grossklags, "What Can Behavioral Economics Teach Us about Privacy?," A. Acquisti et al., eds., *Digital Privacy: Theory, Technologies and Practices*, Taylor and Francis Group, 2007.
13. C.J. Hoofnagle and N. Good, "Web Privacy Census," Berkeley Law, Oct. 2012, http://law.berkeley.edu/privacycensus.htm.
14. J. Podesta et al., "Big Data: Seizing Opportunities, Preserving Values," White House, May 2014; www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
15. "7,500 Online Shoppers Unknowingly Sold Their Souls," Fox News, 15 Apr. 2010; www.foxnews.com/tech/2010/04/15/online-shoppers-unknowingly-sold-souls.
16. A. Acquisti and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," *Proc. 6th Int'l Conf. Privacy Enhancing Techniques* (PET 06), 2006, pp. 36–58.
17. "Big Data and Privacy: A Technological Perspective," President's Council of Advisors on Science and Technology, Report to the President, May 2014; www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.
18. *S. and Marper v. United Kingdom*, ECHR 1581, 4 Dec. 2008.

Frederik Zuiderveen Borgesius is a researcher at the Institute for Information Law at the University of Amsterdam. His PhD dissertation (for the University of Amsterdam) on improving privacy protection in behavioral targeting will be published by Kluwer Law International in the spring of 2015. Contact him at f.j.zuiderveenborgesius@uva.nl.