PUT CONSUMERS FIRST

Data privacy is rightly among the biggest concerns in the digital age but, as **DANIEL SEPULVEDA** argues from the industry perspective, a regulatory balance is needed between protection and the success of a data-driven economy

The recent global rise of law and regulation on data protection has elevated the issue to a high level of public scrutiny and industry engagement. As a result, the time is ripe for the establishment of baseline standards within and across jurisdictions for a set of ethical commercial practices in the collection, use and distribution of people's information.

The advertising and marketing technology industry plays a unique role in these discussions because our businesses rely on accessing consumer data to construct and deliver advertising that is relevant and effective for publishers, advertisers and marketers. Doing that in a way that all consumers can embrace and trust is our responsibility. Today, in the eyes of many consumers and policymakers, we are falling short. What to do?

The marketing industry is a trillion dollar industry, creating millions of jobs, facilitating the flow of commerce, helping sustain communities, financing the global open internet, and enabling free or subsidised access to information and services. At its best, it is undeniably a force for good. And as long as we live in a market economy, advertising is a necessity. At its worst or most poorly managed, it exposes people to harm, unfair discrimination or unwanted attention.

In this article, I highlight principles and ideas that show promise in recently enacted data protection legislation and proposals that empower consumers to protect their digital dignity without disabling commerce. I raise concerns about some assumptions that undergird other components of proposals in recent legal reforms that distort competition, put information in silos, or create unworkable enforcement formulas. I close with recommendations for a way forward.

The objective of my company, MediaMath, and the industry we are in is to ensure consumers grow to love data driven marketing rather than grudgingly tolerate it. To reach that objective, we need to make it better as an experience and update and strengthen self-regulatory data protection standards, empower and educate consumers, and provide directional guidance to legislators for new law or regulation where it is considered necessary or useful.

The EU's GDPR and California's new CCPA: are they flexible enough?

CONSUMERS WANT CHANGE

Confusion, concern and distrust permeate the current market for people's information and the industry needs a new paradigm for public deliberation with policymakers and thought leaders on data protection and privacy. We believe that privacy is human right. That belief is what has driven us to the "consumer first" principle. And we believe that putting the consumer first is also a good principle for deliberation because regardless of whether or not others agree that privacy is a human right, putting the consumer first is a principle that all commercial stakeholders should be able to agree on because a happy consumer is a better customer and more content citizen.

We recognise the challenge to do better and want to work with anyone interested in a better digital future to deliver a better deal to consumers. We also recognise and accept that solutions will require stronger self-regulatory standards, new laws, or some combination of the two.

A vocal bloc of consumers are expressing their dissatisfaction with targeted advertising by adopting ad-blocking technology and pressuring policymakers around the world to pass new data protection laws. In the US, use of ad-blocking technology has gone from 16% of internet users in 2014 to 30% this year.[1] In California, the desire for action on privacy led to such strong support for a very poorly constructed ballot initiative that the legislature was forced to preempt it and pass the most sweeping state law on privacy in the US, the California Consumer Privacy Act (CCPA), by a senate vote of 69 to 0.[2] And in Europe, the use of ad-

blocking technology is the highest in the world and the most restrictive data protection rules for any western market, the General Data Protection Regulation (GDPR), went into effect this year.

It is critical that data-dependent companies meet consumers on terms and conditions that consumers embrace. At the same time, we need to recognise and preserve the value of the data-driven economy and the free and open internet. These goals are not incompatible, but they do require agreed rules and norms for the market as a whole to achieve them.

A recent letter from the Association of National Advertisers (ANA) to the National Telecommunications and Information Administration (NTIA) in the US, regarding potential changes to privacy law, lists the economic benefits of interest-based advertising. The authors cite a Harvard study reporting that the advertising-supported internet ecosystem generated more than a trillion dollars for the US economy and more than 10 million US jobs in 2016.[3] That is real money going to sustain real communities and help people provide for their families.

We should not use public policy to discourage or block the flow of data across the ecosystem because it would come at immense economic costs. But we can and should use it to empower consumers to trade data for services in a transparent and inclusive market, protect consumers from harm or deception, mandate privacy by design, increase the control consumers have over who can access and use their information, and ensure that collected information is properly secured.

CONSUMER FIRST FRAMEWORK

Our test for supporting any specific change to market dynamics through increased self-regulation or new legal regulatory solutions is whether the proposal puts consumers and their interests first and preserves the free and open internet with low barriers to entry and participation. To answer that question, we think about what it is that we want the digital economy to enable and what proposed changes might mean for consumers in terms of increased control over their data, market competition, innovation, and better prices and access to services.

Getting data protection law and regulation right will ensure that people have greater control over their digital identity, participate in an explicit value exchange of data for services, and have their preferences respected throughout the life of their information in the ecosystem. Getting it wrong would lead to a less inclusive digital economy with large, concentrated pools of data in the hands of a few very large firms, and high barriers to entry into the digital marketplace.

BENEFITS OF RECENT ACTIVITY

What Europe's GDPR and most other recent initiatives including the new California act have got right is the need to place consumers at the centre of the digital ecosystem and to let them know and control who in the ecosystem gets access to their data, the volume of data they hold, and the way they use and distribute that data. It is also important that these new measures uniformly require that data be secured and provide for an expert agency or authority with the power and resources to enforce the rights that people should have in the digital economy over their information. Law and self-regulation should not leave consumers to their own devices in a complex marketplace for data.

To the degree that existing self-regulatory programmes do not encompass these principles, they should, as should any new law. Taken as a whole, these provisions make the existing implicit value exchange between the consumer and the array of market actors involved in the stewardship of their data explicit and place requirements on those entities to respect consumer preferences.

AREAS FOR CONSIDERATION

There are some areas where the discussions in various jurisdictions to date have either left some problematic ambiguity or are built on mistaken assumptions.

The free-rider challenge In the GDPR and CCPA there is a central question for the providers of advertising-supported services as to what they can or should do if a consumer chooses to reject behavioural advertising. Both the GDPR and CCPA argue that the privacy conscious consumer should suffer no penalty as a result of that decision. The outstanding question is what constitutes a penalty and whether or not the consumer should be allowed to use the service without payment.

It is our position that if a consumer is going to exercise his or her right to deny monetisation through interest-based advertising, that decision should not be penalised but neither should it be rewarded. The CCPA posits that a service provider cannot deny a service on the basis of a consent choice – but that it can make up the monetisation lost through some other form of compensation. Interpretation of the GDPR and the construction of the EU's draft e-privacy regulation have not made the European definition of "penalty" clear yet.

How best to execute the principle in question is a key challenge that deserves further analysis. The CCPA concept is good in the sense that it recognises that the provision of services is not free and service providers have a right to require some form of compensation if they cannot monetise through advertising. But by stating that the service provider can only charge an amount equal to that of the data lost, it creates a form of rate regulation that will be tough to understand, quantify and police. Further, unless the service is a necessary utility, the service provider should not be forced to provide services to anyone. While access to the internet may be considered a utility, necessity or human right, it is not true that access to all the services made available over the internet fall into that category as well.

First vs third parties First-party collectors of people's information are the companies and websites that consumers deal with directly. Third-party collectors are those that acquire information from a first party or public source and make it available to other parties.

There is an assumption inherent in some privacy proposals that the first-party collection and use of people's data should be preferred and encouraged over third-party collection and use. This may seem intuitive given that in our personal lives we trust people we know personally more than those we do not. While that rule of thumb works well in our personal lives, it is not particularly good for commercial relationships, nor would regulation that prefers first parties to third parties be good for consumers. It would simply empower huge, siloed datasets concentrated in a few companies over access to useful data for new entrants and general market use that when properly regulated is good for consumers.

Neither first nor third parties are inherently better at protecting consumer privacy due to where they sit in relation to the consumer. There are good and bad first-party stewards of data; there are good and bad third-party stewards of data. What matters most in the commercial stewardship of personal ➡

data is not whether the consumer knows the commercial actor but rather what data the actor collects, the context in which it was collected, the sensitivity of the data, how it is used and secured, and to whom it is disclosed and for what purposes.

What law and regulation should encourage is high standards based on fair information practice principles by any collector or user of personal data in the ecosystem, a preference for pseudonymous information, restrictions on data collection and use that could cause harm, and an allowance for the market to reward or punish the quality of data regardless of source. This means that in a transparent market where data holders respect consumer preferences across the ecosystem it shouldn't matter who is holding the data. The existence of third parties and who they are should be made transparent and companies who work with third parties must transmit consents and permissioned uses to the rest of the ecosystem, but there is no logical consumer-first reason to legislatively discriminate against third parties.

By placing a heavy emphasis on providing notice and obtaining consent from people for the use of their data, the GDPR and similar laws in other markets favour first parties, which have the easiest to use and most direct interface with the consumer.

The California law establishes an opt-out mechanism to deny companies the ability to sell consumer data but is unclear on first-party collectors that do not sell consumer data but monetise their first-party data through first-party directed advertising, including behavioural advertising. As Facebook CEO, Mark Zuckerberg, likes to point out, Facebook doesn't sell user data, it sells access to user audiences. The California bill isn't clear if it covers that circumstance or not and if not, why not.

As a result of these constructions, each of these models favours walled gardens within large first-party enterprises over an open ecosystem. Ultimately, that is bad for consumers, competition, and privacy because as you can tell from the problematic cases that we have seen recently, including Cambridge Analytica and Facebook, it is the largest collectors and holders of information as well as disseminators of media through a single platform that pose the greatest risk to consumers of manipulation or harm because they can transmit the most, and most sensitive, information broadly. An American framework should not make this mistake.

Risk of defining pseudonymous information as personally identifiable To recognise, understand and respect consumers, market actors need a mechanism for identifying them. We believe that enabling some form of pseudonymous identification for a unique user across websites and devices is likely to lead to better services and marketing for that consumer than a series of walled off and siloed buckets of data within first-party websites with personally identifiable information (PII) such as the names, addresses, and phone numbers of those consumers. Pseudonymous identifiers allow you to identify a device or consumer without identifying who that person actually is. Though that does not prevent abuse targeted at specific people, it can reduce risk and should be recognised and valued as such.

> **Current models do not have flexibility to allow for exceptions or experimentation with new technologies.**

Encouraging the development of first-party aggregators of large audiences that do not allow for a consistent, tailored, nonrepetitive message for that consumer across touchpoints will lead to consumers being mistargeted or excessively retargeted because marketers will be spending on advertising in buckets of nontransparent data.

The GDPR and CCPA have a very expansive definition of PII that includes pseudonymous identifiers. The incentive that creates is for firms not to go through the work of creating pseudonymous identifiers and to instead collect truly personally identifiable information and distribute it broadly. It is well understood that pseudonymous information can be de-anonymised to get you to a known person but that does not mean it has no value from a privacy perspective and that action can itself be banned or made illegal and should be.

Allowing for flexibility and innovation Lastly, current models including the GDPR and the CCPA do not create enough flexibility to allow for exceptions or experimentation with new technologies that may be in the public interest. The use of artificial intelligence (AI) and blockchain technologies may be hindered by requirements in some of the new laws being enacted. AI allows for automated decision-making by machines using data. The demand to require a specific explanation for each decision would make it difficult to use this new technology. Blockchain technology allows for an uncorrupted ledger of transactions thereby making the right to be forgotten or right to erasure difficult to execute.

The internet of things (IoT), much of which will have no screen or mechanism to convey notice and gather consent, could face similar challenges. And the prescriptive process-based mechanisms for legal compliance designed into the GDPR and the CCPA do not create space for the design of alternative mechanisms through government-approved self-regulatory standards to achieve the same level or compliance with principles through other means, and they should. For the purposes of experimenting with new technologies that may require waiving a right to notice and consent or the right to deletion of information held, there should be some mechanism for petitioning for allowance of use of those technologies on public or legitimate interest grounds as the GDPR allows but for which we have not yet seen specific decisions.

CONCLUSION

Privacy law need not make consumer data off limits to market actors trying to reach them. That would serve neither publishers, consumers, nor marketers. But we do need to make consumer data available on terms and conditions that consumers embrace, permit, and understand. That should be the goal of both updated self-regulatory mechanisms and new law where necessary.

DANIEL SEPULVEDA *is VP for global government relations at MediaMath, a developer of programmatic marketing technology. He was previously ambassador and deputy assistant secretary at the US Department of State where he led delegations on technology and telecoms issues.*

REFERENCES **1** As ad blocker use grows, publishers face new challenges. eMarketer, 26 June 2017. bit.ly/2rStAdt **2** California passes sweeping law to protect online privacy. New York Times, 28 June 2018. nyti.ms/2tGjAaf **3** Association of National Advertisers. Re: Request for comment on "international internet policy priorities". Letter to NTIA, 17 July 2018. bit.ly/2LdgaSI