THE FUTURE OF CONSENT

The coming revolution in
privacy and consumer trust

Ogilvy CONSULTING

caden

CONTENTS

Introduction: The transformation of Big Data

"Black gold" was what they called it. When Edwin Drake, a farmer-turned-railroad conductor, figured out how to extract oil from the ground successfully in 1859, he launched the next stage of the Industrial Revolution.

The American economy raced to meet demand for petroleum products, with California and Texas emerging as leading producers. The automobile industry quickly followed, literally fueled by Drake's discovery and the fact that, in the United States, the precious, black stuff seemed to be everywhere. This was the actual Gold Rush Americans had been waiting for.

Today, we don't glamorize oil and petroleum like we used to. It's still valuable and valued – it funds entire nation-states in some parts of the world – but with the advent of climate change, we've come to see oil and other fossil fuels for the false, dangerous friends they are.

And it only took a century for that reversal to swing into place.

The latest leap forward in the Industrial Revolution has been fueled by a very different source of precious value: data. And unlike fossil fuels trapped in the ground, data is truly ubiquitous. We mine it from human beings. And it's valuable because it not only tells us about them and their behaviors – it can actually shape them.

Like "black gold," Big Data initially enjoyed its own heady days of speculation and astounding wealth generation. It was never just a buzzword, but a divinely ordained call to companies and entrepreneurs everywhere: *Be digitally fruitful, so that your profits may multiply.* It's not for nothing that we capitalize the phrase: a mark of reverence for the sacred promise of data-driven prosperity.

But in recent years, "Big Data" has acquired new associations with invasive marketing, behavioral and political manipulation, and even monopolistic economics. In the United States, especially – one of the epicenters of the financial Wild West represented by the

early days of the Internet – we've culturally rebranded data as a necessary evil.

It's the fuel that powers our modern lives and economy. It creates jobs and makes everything easier. It connects us and allows us to share ourselves with the world. It's created economic opportunity for more people than any other technology in recent memory. We *need* our digital fuel, and we're not ashamed to admit it.

What we're no longer so inclined to accept is the potential misuse and abuse of data at the hands of nefarious actors online *or* the businesses who need it to survive in this brave new digital world. Our law- and policymakers have stepped up, introducing new legislation that protects and empowers consumers to have more control over their data and its usages.

The problem with this approach is that brands, businesses, and other institutions with the necessary digital wherewithal can find ways to work around regulatory protections. Because at the heart of most privacy legislation is a perfectly liberal, laudable principle that envisions all consumers managing their own privacy preferences. This has been referred to as *privacy self-management* (Solove 2012).

It's a principle that hinges on one precious attribute of data, the Holy Grail without which organizations cannot safely and compliantly use the digital fuel they so desperately need: consent.

Consent is the great legitimizer of all data. Once secured, it can justify any number of collection, use, and disclosure practices. In theory, this approach to personal data privacy management makes sense. Rational adults have the right to consent to any number of things in their lives – legal, medical, financial – and the keys to their digital identities should be no different.

In practice, things look very different. Once captured, consent can be used to legitimize practices that would otherwise be deemed illegitimate. Even the original titans of the digital Industrial Revolution – e.g. Facebook, Google, and Amazon – do not have the technological capability to understand the myriad ways in which their algorithms use (or potentially misuse) our data. This "natural" resource is unlike any other the world has seen, and since the Internet began, lawmakers have been wrestling with the question of how to protect us adequately, while still defending our vision of a liberal, open, free-market Internet.

The future of consent will be determined by how we – as individuals, nations, and a global species – evolve our understanding of what counts as *meaningful consent*. For consumers and users, the greatest challenge lies in connecting consent to a mechanism of *relevant, personal control* over their data. For businesses and other organizations, the task will be to recast consent as a driver of positive economic outcomes, rather than an obstacle.

In the coming years of digital privacy innovation, regulation, and increasing market maturity, everyone will need to think more deeply about their relationship with consent. As an initial step, we've assembled this snapshot on the current and future state of (meaningful) consent: what it means, what the obstacles are, and which critical changes we need to embrace to evolve.

Consent is the great legitimizer of all data.

MEANINGFUL CONSENT: SYMBOLIC, INCENTIVIZED, DYNAMIC

Meaningful consent is informed, symbolic, incentivized and dynamic

Not everyone agrees on what consent looks like. In privacy regulation and law, this is perhaps best demonstrated by the differences in the definitions used by the EU and US.

With GDPR, the EU introduced a much more stringent and prescriptive definition of what qualifies as consent, as well as greater restrictions on data collection, use, and disclosure practices. In member EU states, these practices require a demonstrable legal basis before personal data can be processed. In most states in the US currently, the processing of personal data operates more liberally, unless it presents a clear legal problem. With the exception of CCPA legislation (and the tenuous future CPRA) in California and a number of states enacting similar legislation, the US has a less explicit definition of consent.

We all recognize this dilemma from the cookie consent pop-ups that appear on websites we visit. There is enormous variation in how these pop-ups attempt to capture our consent: some are transparent and informative, others are deliberately obscure and make it harder to control personal preferences. The hope in the latter is that users will take the easier route and simply "Accept All" when they land on a page.

What most modern definitions of online consent have in common is the mandate that the consent be *informed*. To understand this, we might look to the fields of medicine, where doctors are legally required to gain informed consent from their patients before operations or other risky procedures.

Technically, it isn't enough for doctors to merely explain a procedure. They must ensure that patients, of their own free will and without undue pressure or control from an external source, understand and retain the information they receive. This is called *information transfer,* more formally.

> *Most entities who have to worry about data compliance rarely engage in any meaningful explanation of what they want users to agree to and how it may change as time goes on.*

Similarly, in digital environments, we should only qualify user consent as meaningfully informed if they can demonstrate a retained

understanding of how their data is collected, used, or disclosed by a given entity.

In medicine, when this is done right, obtaining consent confers greater trust on the doctor and in the doctor-patient relationship. We've all probably experienced this before: when a doctor takes the time to explain something that is easy for them to understand but complex for us, we appreciate the mutual respect this action implies.

In fact, modern medical consent was first formalized in the wake of Nuremberg trials that convicted Nazi doctors who had experimented on Jewish people and other concentration camp victims. These were viewed as crimes against humanity not simply because they were cruel and violent, which obviously abrogates the medical responsibility to do no harm, but also because they undermined the personal agency of patients and medical research subjects.

Obtaining consent in medicine is therefore both practical – it keeps patients informed and doctors protected – and theoretical. We see it as a human right. And because of the power differential between an expert doctor and a layperson patient, when it's done right it can imbue the relationship with added trust, respect, loyalty, and value. This symbolic halo effect is just as important as the practical benefits.

Now, we might easily object that consent in a medical relationship is more easily granted precisely because of that power differential. Online, there's (generally) no risk of death or serious disease. Patients in a hospital or doctor's office often have no other choice than to listen to the advice of a trained professional when faced with something they don't fully understand.

To an extent this is a valid objection, and it demonstrates how *incentivization* is another pillar of meaningful consent. When we introduce consent into human relationships, it's because there is a potential for abuse of power. The patient's interest in their own health and survival incentivizes them to give the doctor consent.

Online, the incentive is frequently to use "free" services, engage with content, or acquire products that are useful (personally, socially,

professionally) to the user. But the difference is many of the online providers of these "incentives" do not accurately represent the risks of using them. Incentivization without information therefore lays the groundwork for abuse of power.

The Cambridge Analytica scandal is the most famous illustration of this: Facebook users participated in data sharing practices that they had technically consented to on the platform, but nowhere had they been informed that a third party might repurpose their data to shape voters' thoughts and behaviors in a political election.

Finally, in medicine and more commonly in biomedical research, consent is *dynamic*. You cannot consent to every surgery simply by consenting to the first one. When a research project studies subjects over long periods of time, they have to regain their consent regularly. Subjects also have the right to alter their decisions at any time. This model of informed consent takes into account the fact that things can change for subjects, as can a study's usage of personal or clinical data.

This doesn't happen often online. Users will consent to their cookies being tracked once on a website and never have to deal with the issue again. Or they'll agree to a Terms of Service document they don't understand and will never read. Most entities who have to worry about data compliance rarely engage in any meaningful explanation of what they want users to agree to and how it may change as time goes on.

02

THE CHALLENGES BEHIND MEANINFUL CONSENT

Understanding the challenges behind meaningful consent

In light of these definitions of meaningful consent – informed, symbolic, incentivized, and dynamic – a number of challenges arise.

First and foremost, how do you obtain informed consent when companies cannot or will not explain the risks associated with their data practices? Unlike heart surgery, enabling cookies doesn't typically present life-or-death stakes. And yet, as we have seen in the past decade on a macro and micro level, there are very real risks associated with exposing your personal information online.

National cybersecurity attacks. Election tampering. Misinformation. Credit card fraud. Financial and health data breaches. Hacking and phishing. Identity theft. These are common, highly damaging risks associated with data use, collection, and disclosure practices. Most people remain willfully ignorant of them, while most companies avoid the subject altogether. The lack of accurate risk assessment inherently makes "consent" theoretically meaningless online.

A related challenge is the transparency problem: companies can legally protect themselves by explaining information in privacy notices and terms of service, but most users don't have the expertise or time to understand these documents adequately. Everyone grows up learning that you should never sign something before you read it, but the Internet forces us to do exactly that every day. The transparency problem is not an issue of user laziness either. One 2008 study at Carnegie Mellon found that the average user would take 76 work days to read all the privacy policies they typically encounter in a year.

Everyone grows up learning that you should never sign something before you read it, but the Internet forces us to do exactly that every day.

Even if companies wanted to be entirely transparent, they can't. Making proprietary technology publicly available by explaining how it works goes against our principles of free market competition. And in the case of algorithmic usages of data in A.I., it can be

extremely difficult to simplify the complexity or adequately explain all the potential risks associated with it. Data scientists and engineers can't always tell how their algorithms will develop in the future, or how datasets containing personal information might be re-purposed.

Which brings us to the final challenge: obtaining meaningful consent can quickly become cumbersome, making it costly both for user attention and companies' bottom lines. Many independent studies have proven that more consent interventions don't necessarily equate to greater consumer understanding or positive outcomes for businesses. In fact, onerous consent practices can often prove blockers to innovation and product or service quality.

As a society, we remain divided on what exactly to do in these situations on both personal and regulatory levels. The problem is clearly illustrated by the case of tools like Consent-o-Matic or Cookie Auto Delete: browser extensions that allow users to "set and forget" their cookie preferences, irrespective of the pages they land on. In theory, these tools are designed to help users reject invasive practices in data storing, collection, disclosure, and usage.

But in practice, does unilateral rejection actually imply meaningful consent? OneTrust, a market-leading privacy and data management firm, thinks not. They recently filed a patent for software that would help detect automatic cookie policy rejectors and deactivate them. But the creators of these tools feel that there are significant differences – philosophical and practical – between refusing consent and granting it.

Both sides of this debate could probably make a fair case. The point is, one of the greatest challenges with consent on the Internet today is that the interactions that grant or reject it are innumerable. Privacy self-management is impractical insofar as it puts the onus on users to manage their preferences at an impossibly granular level. And more prescriptive, universal measures don't necessarily offer sufficient protection or meaningful engagement.

THE THREE PATHS

Three paths to the future of consent: better storytelling, better trust, and better technology

On the surface, these challenges are, if not intractable, extremely complex. What ingredients do we need to ensure that meaningful consent keeps consumers informed, feeling respected and incentivized over time? And how do we ensure those solutions work economically, not just ethically, for the businesses and other entities who serve them?

First – and this is the lowest hanging fruit – we need to engage users with better storytelling. Clear-cut UX/UI practices that lead to more users clicking a green "Accept All Cookies" button is not enough. We need meaningful, informed engagement.

In other industries where personal safety must be communicated, brands have come a long way in this respect. The airline industry evolved from cartoonish plane safety cards with laughably confusing illustrations to big-budget productions that employ humor and vibrant storytelling to grab travelers' attention.

British Airways brought together some of Britain's top celebrities in their plane safety video, making it enjoyable to review the oft-repeated safety instructions we're all mostly familiar with. Virgin Atlantic created a typically whimsical animated story that transformed a dull prelude to air travel into a visually artistic gem. Many airlines have since followed suit. And while it's difficult to prove that these videos actually improve safety outcomes, that's not really what the videos set out to do.

People generally don't pay much attention to safety videos in the first place – nor are they able to retain information from them (one study suggested 53% of people retain information from standard safety videos versus 47% from humorous ones). But these videos have symbolic value: they reinforce the perception of the brand as (quite literally) invested in passenger safety.

Nearly 60% of consumers worldwide say they'd distrust something until they're given a reason not to.

Better storytelling is chiefly critical to securing the symbolic value of consent. If brands and businesses can demonstrate transparency and concern in gaining consumers' consent through relevant communication, they will have won half the battle already. These interventions, when conducted successfully, improve consumer relationships by engendering trust, which in turn leads to better reputation for the brand on a macro level. (And reputation, it has been estimated, is responsible for up to 25% of a brand's market valuation.)

More importantly, it's easier to gain meaningful consent from consumers that already trust you. And this is the second pathway we see bridging the gap between consent today and in the future: better trust.

Consumers are naturally wary creatures in the 21st century, in part because they've been taught to expect poor behavior from brands in the digital economy. Nearly 60% of consumers worldwide say they *distrust* something until they're given a reason not to, according to the Edelman Trust Barometer. This isn't just healthy skepticism – it's outright suspicion.

If many brands are considered guilty until proven innocent, the onus is on *them* to put their best foot forward and change consumers' minds. That means letting go of the traditional, early Internet principle that *enhanced consent* necessarily implies diminished customer relationships.

As discussed earlier, there's evidence to suggest that onerous consent mechanisms can disrupt a business financially and logistically. But there's also evidence that, when presented in relevant, meaningful ways, consent can make business better for both sides of the equation.

A 2019 study conducted in the wake of GDPR at a major European telecommunications

firm found that enhanced consent actually led to increases in data allowances across all categories (though some were more promising than others). Moreover, the telco's business outcomes improved: the marketing department was able to include more relevant leads in its targeted campaigns, and both sales and the ratio of sales to contacts increased.

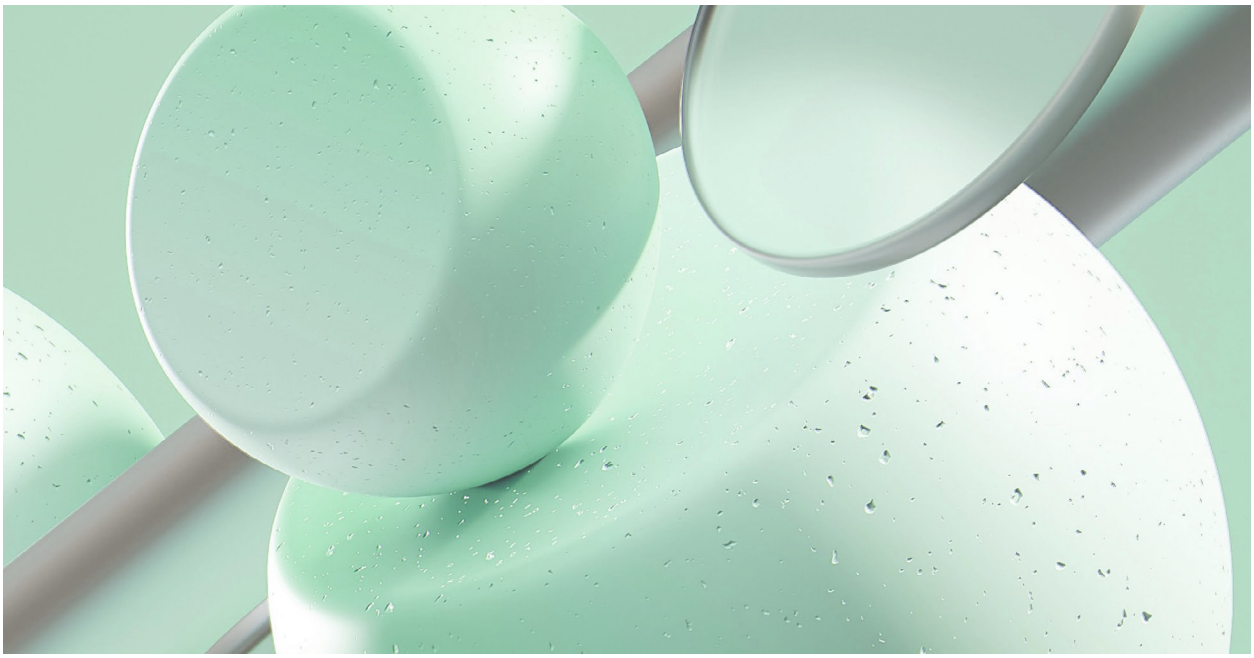
The study worked with over 30,000 households, evaluating the responses over the course of several months for a control group and a treated group (each group containing ~16k households). The control group received a standard form asking customers to opt-in to data collection and sharing practices, while the treated group received a GDPR-compliant form – i.e., a clear, transparent, explicit explanation of the practices the firm engaged in and how they impacted consumers.

If many brands are considered guilty until proven innocent, the onus is on them to put their best foot forward and change consumers' minds.

The largest changes were found in household service usage information like Internet traffic logs, television usage logs, call detail records, and video-on-demand purchases (27.6% of treated households opted in versus 4.3% of the control group). These are all datasets that help the business operate better and improve its products.

Similarly, profile information allowances – e.g. demographics and bundle price/type – increased for the treated group by over 10 percentage points. The numbers were significantly lower for both groups when it came to more intrusive practices like geolocation data and 3rd-party sharing.

Another interesting result was that additional households in the treated group consented to *more* sharing in the months following the GDPR-compliant form. The proportion of treated households who *rejected* consent at all levels decreased from 43% to 28%, implying that a halo effect of the initial communication encouraged more users to trust the telco and opt in.



These results should encourage all brands who are wary of meaningful consent. They demonstrate the upside of building trusted, consensual data relationships with consumers. Provided the data practices are vital to the business or product in a clearly explained way, consumers are mostly happy to share their data. And since more invasive practices are being regulated out anyway, the low opt-in rates for 3rd-party sharing should only deter those businesses who are infrastructurally unprepared for the coming changes.

The one challenge that remains is the question of consumer control and self-management. How can we expect users to toggle their preferences for every brand in every situation?

The answer is, of course, we can't. And this is where the third pathway to the future of consent comes in: better technology for a better experience.

Currently, there are two main camps of technological innovation that are powering us toward new futures for consent.

On one side are the new kids on the block, who believe that decentralized technologies like cryptocurrency and other forms of blockchain data will achieve a permanent revolution in digital trust by *removing* the need for consent and permission. Because they are decentralized and encrypted, blockchain-enabled data relies on an open model of peer verification and public ledgers that never requires recourse to a trusted intermediary.

On the other side are the Web 2.0 veterans who believe that, even without the advent of blockchain and so-called "trustless" technology, we could still build towards a data economy underpinned by meaningful consent. Within this group are innovators working to nudge the data economy – consumers, brands, and all – toward an incrementally different ecosystem.

Neither side is unilaterally right, but the promised revolution of a "trustless" Internet has been slow in coming and remains elusive. Certain industries, such as financial services, have seen exciting, highly volatile periods of growth and opportunity thanks to blockchain technology. But it hasn't been responsible for users gaining greater control over and access to their financial data.

Even amongst the Web 2.0 innovators, there hasn't been a single process that has really helped put users at the center of the privacy experience. Many of the innovations have actually been tactical strategies, designed by technological giants to maintain their competitive advantages

Apple's "Ask App Not to Track" feature for iPhone and iPad, which slashed into Facebook's advertising revenue, has not changed the consumer experience or introduced meaningful consent into its customer relationships. It is in large part designed to shore up Apple's data defenses, and ensure that revenue from app data is funneled through its own advertising channels (unsurprisingly, Apple's App Store ad revenue soared after they rolled out this feature).

Even more recently, Google launched a first-party data sharing system for advertisers and publishers called PAIR (Publisher Advertiser Identity Reconciliation). This is a new form of identification that allows advertisers to target users who've shared their data with them *and* a publisher that has a relationship with that advertiser. Google asserts this system gives the user more control over what ads they see, but in reality, from a user perspective, all it does is continue to serve (slightly more relevant) ads to users in the same websites. It's a perfectly nifty system, which admittedly avoids the exchange of any PII (Personally Identifiable Information), but it doesn't magically create meaningful consent between publishers and users or advertisers and users. It does nothing to improve or deepen the customer relationship.

No one has figured out a system within our current data economy that puts users at the center of their privacy self-management experience.

We need to move on from innovations that merely allow us to do the wrong things in slightly better ways. At the same time, we need to work in ways that don't demand wholesale revolutions in our technological infrastructure. Change comes gradually on the Internet, as with any technology.

The truth is: no one has figured this out yet. No one has figured out a system within our current data economy that puts users at the center of their privacy self-management experience. And that can only mean that we need our technology to provide *low-lift* ways for brands to gain meaningful consent from their consumers. Only when marketers across the ecosystem are able to experiment with this successfully will the tide begin to turn in favor of truly trusting brand-consumer relationships.

CONCLUSION

Conclusion: tracing a path to the future of meaningful consent

The future will be built by brands who invest in meaningfully consensual relationships with their customers that reward them for their trust. Brands who do not build meaningful consent into their customer relationships are already under pressure in massive markets like the EU, US, and Brazil, where privacy regulations are tightening. As a result, the most pressing question every marketer needs to ask themselves about their consumer relationships is: what if we just asked for consent?

At Caden, we're building a personal data engagement platform that centers users and injects consent automatically into brand-user relationships. By giving users more relevant, rewarding control of their data sharing, and by allowing brands to directly incentivize them for deeper relationships, Caden is part of the incremental change revolutionizing the future of *meaningful* consent.

> *Give users meaningful control over what they share and how they are rewarded for it, and the data economy will begin to shift to a preference for built-in consent.*

We don't believe that we're going to solve everything in one fell swoop. Our mission is to create proof points for brands, consumers, and the many experts studying the future of privacy to show that enhanced consent leads to better

outcomes for all. If Caden can serve as a digital "consent key" between businesses and their targets, we believe we can begin to point towards a future where meaningful consent is the gold standard of brand-consumer relationships.

That consent must always be informed, dynamic, symbolic and incentivized.

Informed does not mean throwing technical and legal jargon at users: it means communicating – through clear, impeccable storytelling – relevant explanations of data practices that actually mean something in users' daily lives.

Because of the changing and unpredictable nature of data practices, particularly with the acceleration of AI, meaningful consent also has to be dynamic. That is, brands and businesses have a responsibility to renew consent when and if their data use practices evolve. This creates *more* trust and better relationships over time – not less.

That last point is related to the symbolic nature of meaningful consent. When users are involved in an informed, dynamic, consensual relationship, they feel respected and respectful. They are far more likely to put their trust in entities who treat them like intelligent, responsible human beings. As David Ogilvy once said, "The consumer is not a moron." Brands who continue to labor under the impression that users are too busy or too incompetent to appreciate meaningful consent will continue to create brittle, short-lived consumer relationships.

Finally, meaningful consent must be incentivized. While the symbolic value of a consensual relationship is powerful, we all know users prefer paths of least resistance. Incentives – such as loyalty rewards, more relevant communications, and better products and services – are a fantastic way to get users locked into the new normal of meaningful consent. But these incentives have to be relevant to both the business, consumer and their relationship. Extra bits of crypto and junk swag won't cut it. Users want meaningful rewards if they're to provide you with meaningful, valuable information about themselves.

On the surface, it seems like there's an incredible amount of complexity intrinsic to the consent and privacy challenge. But one thing is clear: the future of consent, and therefore the future of consumers' relationships with brands, depends on an incremental approach. Give users meaningful control over what they share and how they are rewarded for it, and the data economy will begin to shift to a preference for built-in consent.

As data becomes heavier and costlier to manage, brands will be forced to embrace more elegant solutions that serve users and lighten their economic and compliance load. If we can achieve a one- or two-degree turn in that direction, with a low-lift, low-friction and high-value experience, then it will become obvious to both sides of the marketplace that a future built on meaningful consent is not only brighter, but far more desirable.

Because in the coming century, the most precious digital "gold" will be the data people actually *want* you to have.

Acknowledgements

CARLA HENDRA
Global CEO, Ogilvy Consulting

Carla Hendra is the Global CEO of Ogilvy Consulting and has been at the forefront of strategic innovation for brand and business for over 25 years. Carla lives in New York City.

Ogilvy Consulting is the strategy, innovation, and business insights arm of The Ogilvy Group. An enterprise-wide offer, we provide advisory services across Business Growth & Innovation Strategy, Business Transformation, Brand & Marketing Innovation, Sustainability, Behavioral Science & Futuring.

Ogilvy CONSULTING

JOHN ROA
Founder & CEO, Caden

John Roa is Founder & CEO of Caden. He is a lifelong entrepreneur, technologist, philanthropist, investor and author. John lives in New York City.

Caden is debuting the first Open Data platform. To date, brands collect first-party, second-party and third-party data on consumers to create internal Consumer Data Platforms, creating siloed profiles of each user. The Caden platform breaks down those walls, allowing for users to collect various forms of disparate data from the brands that they interact with in their digital lives. In this "zero-party data" future (defined as demographic, behavioral or preferential data a user willingly shares with a brand for a value exchange), brands will be able to provide a more personalized and context-driven experience, with the user squarely in the center.

caden

This is the last in a series of three papers on the future of data, privacy, technology and brands jointly published by Ogilvy Consulting, the global innovation arm of the Ogilvy network, and Caden, an open data startup creating new consumer products to empower both customers and brands.

Sources

- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7163223
- https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3777417
- https://ahrecs.com/resources/ai-big-data-and-the-future-of-consent-papers-adam-j-andreotta-et-al-august-2021/
- https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_solove.pdf
- https://docs.google.com/document/d/19jQEtZxMe54lIDGEdFh5q9DhyZoSLGc_Y5T8N7yjyI8/edit
- https://www.vice.com/en/article/y3p5q5/open-source-consent-o-matic-tool-lets-anyone-automatically-stop-websites-from-tracking-them
- https://dl.acm.org/doi/10.1145/3491101.3519683
- https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/
- https://www.nature.com/articles/s41431-022-01160-4
- https://www.theverge.com/2016/3/7/11173010/verizon-supercookie-fine-1-3-million-fcc
- https://digiday.com/sponsored/how-brands-are-gaining-an-edge-by-prioritizing-trust-and-consent-in-their-ux/
- https://www.smashingmagazine.com/2021/03/state-gdpr-2021-cookie-consent-designers-developers/
- https://iapp.org/news/a/yes-how-opt-in-consent-really-works/
- https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through-2024
- https://www.theatlantic.com/technology/archive/2017/06/online-data-brokers/529281/
- https://www.adexchanger.com/investment/what-the-end-of-days-for-ad-tech-might-look-like/
- https://www.onetrust.com/company/about-us/
- https://chrome.google.com/webstore/detail/consent-o-matic/mdjildafknihdffpkfmmpnpoiajfjnjd/related?hl=en
- https://www.wired.co.uk/article/korean-air-k-pop-safety-video-superm
- https://www.edelman.com/trust/2022-trust-barometer
- https://inrupt.com/
- https://www.forbes.com/sites/oluwaseunadeyanju/2022/09/01/blockchain-data-is-the-next-big-thing-in-web3-according-to-this-expert/?sh=656ab5621f36
- https://ieeexplore.ieee.org/document/8935049
- https://iapp.org/resources/article/decentralizing-privacy-using-blockchain-to-protect-personal-data/
- https://blog.google/products/marketingplatform/360/engage-your-first-party-audience-in-display-video-360/
- https://www.adexchanger.com/podcast/the-big-story/the-big-story-ad-tech-ripples-from-signal-loss/
- https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes
- https://www.insiderintelligence.com/content/apple-ad-revenues-skyrocket-amid-its-privacy-changes
- https://permission.io/

For more information, please visit us at:

www.ogilvy.com/work/consulting

www.caden.io

Ogilvy CONSULTING

caden