WARC

What we know about data ethics

WARC

Explores consumers' increasing concern about privacy and data protection and how companies can rebuild trust by proactively embracing data ethics in an era where the Internet of Things and smart cities heighten privacy issues.

Consumers are increasingly concerned about privacy and data protection and more negative about digital advertising, the tech industry and negative societal impacts they have created. The spread of generative AI, facial recognition technology, the Metaverse, the Internet of Things and smart cities could only heighten the issue. Governments are starting to respond but, beyond regulatory compliance, companies can rebuild trust by proactively embracing data ethics.

Definition

Data ethics goes beyond compliance with personal data protection laws. It is the responsible and sustainable use of data, which does the right thing for people and society. It addresses moral problems related to data and algorithms, which have potential to cause harm.
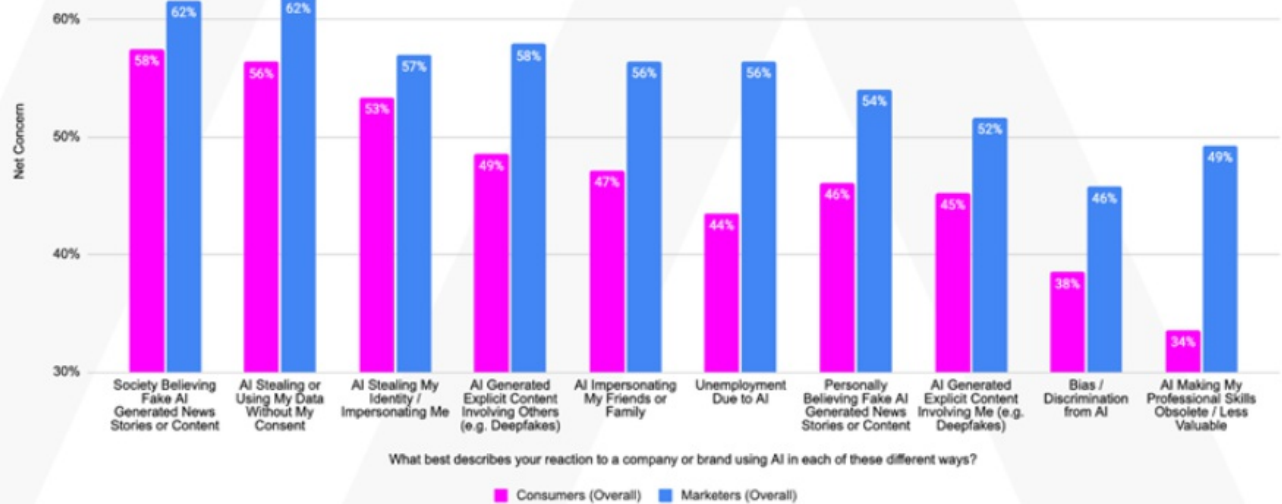
Key insights

1. **The Gen-AI web exacerbates and creates a number of data ethics challenges**

While consumers and marketers are most concerned about AI fooling others or impersonating them, **AI stealing or using their data without consent is also a very real concern** with regard to companies or brands.

AI Fooling Others & Impersonation Are Biggest Concerns

Both Consumers & Marketers are most net concerned about the impact of AI in fooling others or impersonating them - balancing the belief that AI is incredibly capable with the personal attitude that individuals won't be fooled personally by AI content

	Consumers (Overall)	Marketers (Overall)
Society Believing Fake AI Generated News Stories or Content	58%	62%
AI Stealing or Using My Data Without My Consent	56%	62%
AI Stealing My Identity / Impersonating Me	53%	57%
AI Generated Explicit Content Involving Others (e.g. Deepfakes)	49%	58%
AI Impersonating My Friends or Family	47%	56%
Unemployment Due to AI	44%	56%
Personally Believing Fake AI Generated News Stories or Content	46%	54%
AI Generated Explicit Content Involving Me (e.g. Deepfakes)	45%	52%
Bias / Discrimination from AI	38%	46%
AI Making My Professional Skills Obsolete / Less Valuable	34%	49%

What best describes your reaction to a company or brand using AI in each of these different ways?

The Gen-AI web threatens to exacerbate existing issues such as monetising harmful content, data privacy violations, AI bias and ad fraud. It also creates risks related to bad actors and scammers creating deep fake content and potential copyright issues. Working with Gen-AI web companies that adopt a responsible and ethical approach to building and utilising Gen-AI tools will reduce harm, and help minimise risk to brands, and their customers. Working with detection and verification technology firms, influencing the models underpinning AI and investing in premium media can also help brands manage the **risks**. Some practitioners, including Oliver Feldwick, head of innovation at The&Partnership have **called for the advertising industry to embrace AI ethics** and properly interrogate how Gen-AI tools work, the data they are using and the implications for the industry, and society, including biased, illegal or discriminatory work and the unintended consequences that might arise.

Read more in: ***The Gen-AI web: 4 important considerations for marketers*** *and* ***Generative AI: The next creative revolution has already begun***

2. Web3.0 is an opportunity in ethical data use

Customer data has never been so widely available and in such large volumes and data privacy has never been more important. How to harness data ethically while protecting privacy is, therefore, a major challenge for brand owners. Around the world, efforts to upgrade rules on digital services, privacy, and emerging technologies such as artificial intelligence (AI) are stepping up. But at the same time the internet is evolving to a decentralised model, known as Web3.0. This third incarnation of the internet, is expected to be a more decentralised version of the internet, with internet applications and services powered and controlled by distributed ledger technology – the most common being blockchains – and where people have control over their data. It is hoped it will be more open, more accessible and more transparent. While Web3.0 will allay some privacy concerns, new regulatory privacy frameworks will be needed for a world where personal data becomes a well-understood, valued

commodity that also takes into account developments in Machine Learning and AI. Brands are advised to take three actions:

- *Be transparent, open and build trust* – build services/solutions that are genuinely useful and customers are willing to trade their data for; be open about what data is being captured, when and how it's used; give users control; own and quickly address negative situations.
- *Be a leader in regulation* – sticking to whatever regulations are in place at any time is table stakes; brands should see this not as a burden but as an opportunity to differentiate themselves from their competition, by acting as a customer champion; be prepared to guide and influence the development of the regulatory framework.
- *Be a Web 3.0 pioneer not a follower* – design not just for the world as it is now but put in place key building blocks that help navigate the next five to ten years; then invest properly in innovation, treating Web3.0 as an opportunity rather than a risk.

Read more in: **Privacy, regulation and Web3.0: What marketers should consider in 2022**

3. The metaverse quickly needs to tackle data ethics

The metaverse is the next arena where data ethics need to be tackled as people will want their data protected and need to be able to trust the people protecting it. Bearing in mind most companies track customers for marketing purposes and that the metaverse will provide untold new ways of monitoring and tracking individuals, ethical considerations of what is right and what is necessary need to be discussed sooner rather than later. Decentralised systems where consumers own their own data may be a solution, although a potential headache for platforms and regulators. Clear intention and transparency, as well as a desire to work as a global metaverse community, and appreciating that needs will differ wherever you are, will be key to earning trust.

Read more in: **Tensions in the metaverse and what they will mean for brands**

4. AI is a very powerful technology which should be used responsibly to "do no harm"

AI is **most often used by marketers** for product or content recommendation, customer segmentation, social listening and sentiment analysis, search, predictive analytics/forecasting and personalisation as well as to power personal assistants and news feeds. However, AI is not infallible, and its use can go wrong. Due to its unprecedented capabilities, marketers must prioritise responsible use of AI. **Four common challenges** that marketers face regarding AI ethics are:

- Avoiding creation of a systemic unfair advantage
- Minimising unconscious bias due to bad data or assumptions which can create unintentional harm
- Anticipating unintended consequences
- Preventing unethical usage to manipulate and do harm

Bias in AI is a systematic inaccuracy in the representation of reality imprinted within AI systems, due to the prejudices present in their human creators or the data used for training it. However, handled properly, AI can actually be a huge positive in helping marketers avoid bias in their communications and ensure brands serve every consumer. Organisations should scrutinise their datasets for representation and balance, ensuring that they're not favouring one demographic over another. AI models should be trained and tested with data that reflects the broad and diverse range of consumers, ensuring that every person, regardless of their background

or identity, feels seen and valued by the marketing content they encounter. The most critical element in ethical AI practices is transparency, which allows both the creators and the users of AI to see the data that builds the system. This means opening the black box of AI, explaining how decisions are made, and making it clear when AI is in use.

As in recent years, the research industry has launched many new products that are facilitated by AI, including sampling, coding, data collection and visualisation, there is a need for market researchers to earn the trust of survey participants and legislators to retain the industry's ability to self-regulate. Some practitioners have proposed **an ethical framework for AI in market research** based on five principles: AI in market research should be used for good; AI systems should do no harm; there must be human oversight of AI systems; AI systems should promote prosperity and avoid unfairness; and AI systems should be explainable, and developers and users held accountable for the outcomes of AI

The events of 2020 raised concerns about **algorithmic bias, unfairness and unintended consequences**. It is therefore crucial that the design of an algorithm should never be divorced from its intended use and that those designing it combine their technical expertise with human empathy, emotion and understanding. Many organisations, from **Microsoft** to **The Algorithmic Justice League**, have advocated the need to build inclusive teams from diverse backgrounds, cultures and disciplines to design and engineer algorithmic experiences. There are also **universal principles that can be applied to marketing and media**:

1. *Define clear ethical standards that inform AI design* that a company holds themselves, their data collectors, product developers and the rest of their employees accountable to.
2. *Avoid biases in data collection and the machine learning pipeline* as from study design/hypothesis formulation to data processing and collection, model development and model interpretation, both statistical and cognitive biases can emerge at each stage.

Human	**Fairness**	**Security**
Respect human rights, diversity, and the autonomy of individuals, benefiting future generations.	Inclusive and accessible, and should not involve or result in unfair discrimination.	Respect and uphold privacy rights and data protection, and ensure the security of data.
Transparent	**Contestable**	**Accountable**
Responsible disclosure so people understand when they are being significantly impacted by AI.	There should be a timely process to allow people to challenge the use or outcomes of the AI system.	Enables human oversight, people engaged in different phases of the AI system should be identifiable.

This applies equally to algorithms used in **hiring decisions** as to those used in marketing applications. Ensuring diverse decision makers in the process can help avoid or counter algorithmic biases.

In early 2020, tech giant **Google** called for – and offered to engage in - supra-national regulation of AI in a rejection of market forces deciding how the technology should be used. It suggested the framework should consider safety, explainability, fairness and accountability. Meanwhile, **Chinese tech giants have attracted criticism** over their use of algorithms and artificial intelligence, which the China Consumers Association (CAA) says are placing consumers at an unfair disadvantage. This has come amid a broader national conversation

about how tech giants use technology to control information and leverage access to personal data for commercial gain.

Read more in: **Considering the ethical challenges of artificial intelligence bias**, **Do androids dream of electric research?**, **Ethical AI: How to stop marketing efforts becoming a racist, sexist or ageist monster**, **Algorithmic fairness must be at the heart of the tech we design**, **Data ethics: Admap summary deck** *and* **The importance of ethical AI**

5. The move to conscious media investment is helping address unethical data use

While data-driven digital marketing was intended to deepen relationships with consumers and serve them better, it has ended up undermining consumers' trust when companies have misused or not taken care of their data or have not been transparent about its use. The online advertising ecosystem's trading of consumer data and tracking of consumer behaviour undermines consumer data protection and privacy. But beyond that, advertising's funding of the internet has wider repercussions – facilitating the spread of fake news, the creation of biased echo chambers where divisive ideas can go unchallenged and the undermining of democracy through bad actors targeting messages to influence elections. All underpinned by the dominance of Google and Facebook in the data economy. Concerns have helped fuel growing interest in **conscious media investment**.

For example, GroupM, the media investment arm of agency holding company WPP Group, with its "Responsible Investment Framework" is drawing on five key principles as it makes spending decisions for the benefit of its clients. One of the principles is responsible data use, which requires thinking and discussion about the impact of data-related decisions on the individuals whose data is being used. This is operationalised in Group M's **Data Ethics Compass** tool which uses a "proprietary scoring logic", developed in partnership with consumer packaged goods giant Unilever, to rapidly assess the ethical risk levels associated with data assets and decisions through the consumer's lens.

CAN's Six manifestos

How and where conscious media investment makes a difference

Anti Ad-Fraud

Ad-fraud should be eradicated.

Diversity & Inclusion

The industry, the content it produces, and the media it invests in should be as diverse as society.

Informed Consent

Consent should be informed and people seen as active participants in their online experience.

Hate Speech

Hate speech should not be inadvertently funded by brands.

Children's Wellbeing

Advertising to children should be age appropriate, promote positive messaging and values and avoid glamourising particular behaviours.

Mis/Disinformation

Advertisers must take the responsibility to ensure they don't invest in channels that fund disinformation or misinformation.

Source: The Conscious Advertising Network, 2021

Source: The WARC Guide to Conscious Media Investment

Read more in: Can responsible media investing be operationalized?, Data ethics: Admap summary deck, We don't understand how dangerous we are and The relationship between Fake News and advertising: Brand management in the era of programmatic advertising and prolific falsehood

6. Industry initiatives and regulation are reducing the tension between personalisation and privacy

While studies show personalised experiences can increase consumer engagement and purchasing, the RSA Data Privacy & Security Survey 2019 found **people do not want personalised services at the expense of privacy** – just 17% of respondents viewed tailored ads as ethical. The idea of the Personal Data Economy which has emerged in the wake of data protection and privacy legislation holds the promise of non-creepy personalisation because the individual is in an equal relationship with the brand – based on transparent data use, informed consent and mutual benefit.

The demise of third-party cookies, Apple's App Tracking Transparency (ATT) policy, and global data privacy

regulation are combining to **undermine the foundations of personalised digital advertising**. While there are **many advertising ID solutions on the market**, the majority of which aim to identify individual users and share insights into their online behaviour, there are questions about the viability and scale of such schemes. While consumers want relevant communications, there are plenty of ways to reach people without identifying specifically who they are. Furthermore, evidence shows that less user-level data does not necessarily mean less effective. An **IRI study** found that reducing the availability of Apple device ID data did not lead to a fall in product sales.

While there remain **data privacy question marks** about some of the solutions in Google's Privacy Sandbox, **the company is very clear it will not build or use alternative identifiers to third-party cookies** to track individuals across the web because they do not meet consumer's increasing privacy expectations and may fall foul of rapidly evolving privacy regulation. Google's current lead proposal is **Topics API**, which uses machine learning to process data on a person's device. It enables Google Chrome browser to identify up to five interests (topics) that people have the highest affinity for, without an ID.

On the other hand, **Facebook is championing personalisation in a privacy-compliant manner** as it believes emerging technologies will enable the best of both worlds, in which users can maintain data privacy, while brands can continue to target communications at relevant audiences. The platform suggests three innovations may be key to achieving this goal:

- Secure Multiparty Cooperation (MPC): an evolution of data modelling, in which two (or more) companies can combine to aggregate and analyse statistics without exchanging data
- Blind signatures: the use of cryptography to transform an event into something new, which cannot be linked to the original.
- On-device learning: similar to Google's Privacy Sandbox proposals, personally identifiable information (PII) remains on the user's device. This would allow off-Facebook behavioural data to be combined with in-app/on-site behaviour, without that data ever "touching" a Facebook server.

There are also alternatives to hyper-targeted or behavioural advertising – internet search engine **DuckDuckGo** has built a successful and profitable business using keyword-based advertising as its primary business model.

Read more in: ***How to use data in an ethical way: Empower the consumer****,* ***Data ethics: Admap summary deck****,* ***It's time for marketers to reframe personalisation for a privacy-centric era****, The WARC Guide to The future of identity*** *and* ***Google and Facebook offer very different visions for the future of privacy and personalisation***

7. Using data for political ad targeting divides opinion, for some is unethical

The 2018 Facebook/Cambridge Analytica data-privacy scandal focused mainly on the data harvesting of 87 million of the platform's users without correct permission. However, it also highlighted the use of data and psychological profiling for political ad targeting, which is controversial with many consumers, tech platforms and industry practitioners.

According to a Gallup poll ahead of the 2020 presidential election, 72% of Americans – regardless of political allegiance – said internet companies should not release any data about users to political campaigns wanting to target voters with ads. However, one in five were in favour of allowing campaigns to have limited and broad details, such as a person's gender, age and zip code. Revealing this limited information fits with Google's

current policy. Only 7% of people backed the idea that there should be no restrictions on what data is available to political campaigners, a view that is in line with targeting policies at Facebook.

In the run up to the 2019 UK General Election, Twitter banned all paid-for political advertising globally, apart from subjects such as voter registration. Its rationale was that political message reach should be earned not bought by forcing highly optimised and targeted messages on people. This prompted the Institute of Practitioners in Advertisers (IPA), a UK industry body, to urge all online platforms to commit – in the absence of regulation - to a publicly available register of all political ads and ad data online or to follow Twitter's lead. It cited the importance of public, open, collective political debate which it believes micro-targeted political ads circumvent.

Some suggest the use of data in machine-learning algorithms to serve content and recommendations risks humans outsourcing their critical thinking. And that this is particularly problematic when it comes to elections, with individually targeted advertising undermining their fairness unless better monitoring systems are put in place.

*Read more in: **Most Americans say no user data should be released for political campaigns**, **Twitter bans political ads as UK consumers urge regulation** and **Get some recommendation therapy***

8. Psychological targeting seen as not unethical by nature

Psychological targeting uses someone's digital footprint to infer personality which can predict things about them and provide insight to target different messaging. While the Facebook/Cambridge Analytica scandal has shaped negative views of psychological targeting, practitioners argue that it is not fundamentally unethical. Patrick Fagan, former lead psychologist at Cambridge Analytica, suggests it is not the usage of the tool but who is using it that leads people to find it unethical or not. Furthermore, he argues that it is no worse for society than traditional advertising. For him what is important is to give people more power to opt out of ads and to have control over how their data is used and what types of ads they see. Professor Sandra Matz, a computational social scientist at Columbia Business School, suggests that all communication in interpersonal relationships is tailored to some extent and that psychological targeting just mimics this in the online world – enabling brands, companies or political parties to nurture deeper, more personal relationships with people. This can be used for good, for example, to engage more people in politics and enhance democracy.

However, she does acknowledge that using data made public by an individual in a specific context to infer information, such as sexual or political orientation, that the owner never intended to reveal is problematic. And willingness to share data in order to receive personalised advertising for their favourite sporting events, for example, does not mean they are happy to do the same in the context of political campaigns. Regulation that directly addresses psychological profiling, perhaps restricting its use in certain contexts such as political advertising, may therefore be required.

*Read more in: **Can psychographic targeting techniques be used ethically?** and **How psychological targeting can be used for good***

9. Companies are under pressure from consumers on data ethics – especially social media

A **2023 survey by ad-targeting business Nano Interactive** found that UK consumers are increasingly

concerned about giving up personal data and are not convinced by the industry's value-exchange argument. It found that, on a weekly basis, 70% are accessing the internet in ways which mask their personal information e.g. browsing in private or incognito mode, using Safari as their main browser, regularly clearing their cookie cache, and opting out of cookies on websites. When asked why they have become more conscious about online privacy in recent years, ad tracking was cited as the number one reason by 42% of respondents - more than data breaches (31%) or being targeted by online scammers (31%).

A **2023 study by the Pew Research Center** found that three-quarters (77%) of Americans have little or no trust in leaders of social media companies to publicly admit mistakes and take responsibility for data misuse. A similar proportion (76%) do not trust leaders of social media companies to not sell personal data to others without consent. There is particular concern about social media sites knowing personal information about children and the impact of AI on data protection and privacy.

According to Dentsu Aegis research, less than half (45%) of global consumers trust organisations to protect the privacy of their personal data while a similar number **(44%) have taken steps to reduce the amount of data they share online**. 80% say they would stop doing business with an organisation that misused their data – **the leading cause of distrust of the tech industry**. A study conducted by YouGov found that over 90% of global consumers expect brands to use technology ethically and governments to intervene if they do not, with 84% fearing their personal data is not secure. A different YouGov study reported that just **over half of global consumers want to see more regulation** of tech and social media companies. When it comes to advertising, consumer acceptance of display ads on websites in return for access drops significantly – **from 63% to 36%** – once they understand how personal data is shared with advertisers and used to serve targeted ads.

Facebook, Twitter and Instagram are the technology companies consumers trust least with their personal data. Just two-fifths (41%) of respondents to a US survey said they trust Facebook, a number that rises to only 43% for Twitter and 46% for Instagram. Furthermore, globally **23% of Facebook users say they have considered leaving the platform** – driven in part by concerns about data privacy.

*Read more in: **Ad tracking drives privacy push, Data privacy vexes Americans, Consumers reveal their digital concerns, Consumers demand ethics alongside innovation** and **Awareness of data-sharing knocks public support for ads***

10. Companies need to embed data ethics in their organisations to build trust

Making data ethics part of corporate culture is an investment in long-term relationships with customers and stakeholders yielding increased market share and ultimately stronger shareholder value. Embedding ethics is a long-haul game. It requires commitment and a substantial amount of demonstration to shift attitudes, strategies and measurement. Although time consuming and costly, it's the kind of change that can provide a brand with the image and safety-net it needs to build trust and succeed.

For example, **Apple** is seeking to make data privacy a major point of brand differentiation, underpinned by a focus on data protection and supported by privacy engineer and privacy lawyer involvement from the start of every new product design project. The Conscious Advertising Network suggests six areas companies should work on for a more ethical approach to data-driven marketing, which tackle ad fraud, diversity, informed consumer consent, hate speech, fake news and child wellbeing. The World Federation of Advertisers (WFA) has published the **world's first guide for brands on data ethics in advertising** – Data Ethics – The Rise of Morality in Technology – which sets out four key principles marketers need to consider so that their organisation always uses data ethically:

- *Respect:* all usage should respect the people behind the data and use it to improve their lives
- *Fairness:* usage should be inclusive, acknowledge diversity and eliminate bias
- *Accountability:* open and transparent data practices backed up by robust governance
- *Transparency:* open and honest data practices, particularly as AI and machine-learning approaches start to automate decisions

Read more in: **Data ethics: Admap summary deck**, **Potential implications for marketing, measurement and ROI in a post-GDPR world** *and* **Marketers must be proactive to safeguard brand reputation**

11. The forecast growth of the Internet of Things will put further focus on data ethics

The Internet of Things (IOT) is the network of physical devices, like buildings and watches, that have sensors and network connectivity embedded in them. It is facilitated by technologies like 5G mobile connection, AI and voice computing – and fuelled by data. Increasingly intelligent devices can interact with each other, and even make decisions, without the need for human intervention. Active IOT connections are forecast to triple between 2018 and 2025 to reach more than 21 billion – accounting for almost two-thirds of all connections. The growing ubiquity of digital solutions in everyday life will only serve to heighten concerns about privacy, data protection and ethical use of data.

A recent study by Accenture, the consulting firm, found consumers are suspicious of emerging technologies that promise to make their lives easier while collecting more data about them. More than 76% expressed discomfort with data collection through microphones or voice assistants. Also, connected devices such as Google's Nest thermostat, Amazon's Alexa and Facebook's Portal TV can gather rich consumer data and are increasingly common in private spaces such as peoples' homes or cars. Yet, often they have opaque and questionable privacy settings. US lawmakers have already scrutinised consumer privacy concerns related to smart TV tracking. Marketers engaging in emerging tech should review how they are using consumer data, and ensure they are compliant with data privacy laws.

Read more in: **Marketer's Toolkit 2020: Privacy-first marketing (Policy)**, **CES 2019 heralds a shift from the "connected age" to the "data age"** *and* **IoT connections to triple by 2025**

12. Facial recognition technology is a particularly sensitive area, already attracting governmental scrutiny

The launch of the iPhoneX in 2017 brought facial recognition nearer the mainstream. However, consumers have reservations about the technology. A UK survey found that two thirds of consumers were comfortable with the idea but more for use in security than personalised marketing or advertising purposes. In the US, while 56% of Americans trust law enforcement's use of the technology, according to **Pew Research**, just 18% said the same of advertisers. And in China, 74% of respondents to a survey wanted the option of traditional ID, despite a majority also believing that the technology makes transport centres, schools, malls, and condos more secure.

The technology is of particular concern to privacy campaigners who advise marketers of the need for the highest possible privacy protection, the critical importance of positive consent and transparency about the benefits consumers will receive in return. Data protection watchdogs in the UK and Sweden have already taken a keen interest in privacy issues raised by use of the technology and it is reported that the EU is drawing up new legislation to strengthen citizens' rights over use of their facial recognition data.

A draft EU paper proposes a ban on the use of facial recognition in public places for up to five years while researchers and policymakers get their heads around the technology. Concern stems from consent to the use of the technology, which in a public space is unlikely to be willingly given. Also, the technology has been shown to be often inaccurate for people of colour and women, **according to WIRED**. Industry opinion on the EU proposal is split, with Google in agreement but Microsoft not.

Read more in: *Google, EU seek facial recognition pause*, *UK consumers open to facial recognition for security purposes, but less so for marketing - for now*, *Trend Snapshot: Facial recognition* and *EU plans to clamp down on facial recognition*

13. Smart cities should be designed with citizen privacy front and centre

Cisco defines a smart city as one that adopts "scalable solutions that take advantage of information and communications technology to increase efficiencies, reduce costs, and enhance quality of life". Smart cities provide opportunities for brands as well as public service providers, as smartphones connect consumers to the network and generate data on their needs, demands and patterns of life. However, the growth of tech-enabled urban solutions needs to be done in an ethical way – designed for citizen privacy, e.g. by de-identifying all data at source, compliant with data protection laws and transparent in their use of data. Otherwise, the risk is consumers feeling "creeped out" or worse under surveillance.

Read more in: *Drivers of change in 2019: Admap summary deck*, *Smart cities and out-of-home advertising*, *An operating system for the modern megacity* and *Smart cities of surveillance*

14. Data-privacy issues are focusing the research industry on data ethics

In 2018 Facebook was involved in a data-privacy scandal connected to Cambridge Analytica, a UK-based data company, which harvested the data of 50 million of the platform's users without correct permission. This prompted the Advertising Research Foundation (ARF) to create a new code of ethics for consumer data collection and protection. With the technology of data collection evolving rapidly, some organisations are using questionable practices and paying insufficient attention to good consumer data practices. The code will be grounded in four key principles: honesty, integrity, transparency and a chain of trust. The latter is particularly important in the big data era to inspire confidence that data has not been obtained in an underhand way.

Read more in: *ARF slams Cambridge Analytica, drives toward new codes and standards for research*, *ARF probes personal-data use*, *"Fake" research drives ARF to build new code of conduct* and *The ARF seeks a new ethical code for market research*

More on this topic

WARC Topic Page: **Big Data**

WARC Best Practice: **What we know about data protection and privacy**

WARC Best Practice: **What we know about GDPR and EU data law**

Further reading

AI fear and AI ethics: Decathlon explores the knots

Responsible Marketing Frameworks don't cover all the issues

How generative AI redefines interactions between businesses and consumers

Spotlight US: How US marketers are starting to use Gen AI

Spotlight Australia: **Championing privacy in marketing: How culture change impacts strategy**

CMOs struggle to get to grips with data ethics

The future of the internet is about more than third-party cookies

Why corporate morality will define the next step in the evolution of digital marketing

We need to talk about data

WARC