FUTURE AGENDA
Open Foresight

THE WORLD IN 2030
Hidden Organisations of Influence

Hidden Organisations of Influence

The growth in globally influential, yet unaccountable, organisations that are able to undertake surveillance, steer agendas and shape government policy has wider impact.

Photos held by Clearview AI[1]	**3 billion**
Customers of 23andme[2]	**12 million**

In theory it has never been so difficult to remain below the radar. 24/7 news, constant surveillance and demands for greater accountability make it is seemingly impossible for any corporate, political or, on occasion, personal activity to go unnoticed. And yet widespread concerns about the number of increasingly influential, unaccountable, commercially driven organisations that are operating with rapidly expanding reach were often expressed during recent workshops. True, wealthy individuals and organisations have long had a disproportionate influence over elected representatives but the amount of money some companies now have to spend is unprecedented. Furthermore, new technologies have made it easier for others to access information, exert influence and move funds around the world in ways which are almost impossible to trace. The truth is they can operate effectively and invisibly without being restricted by the traditional checks and balances. At a time when calls for greater transparency are escalating it seems that meaningful oversight is lacking.

Secretive Organisations

Operating out of sight is nothing new. Indeed, many organisations have intentionally kept a low profile. Most governments have a network of covert operations tasked with keeping the country safe by the collection and analysis of human intelligence. These activities, often brought to life in books and films, are a vital part of protecting the nation. In fast-moving markets, where protecting intellectual property is a priority, being secretive is a necessary part of the strategy. Many successful brands have therefore chosen to keep their internal activities and strategy hidden - KFC, Coca-Cola and Mars are all good examples. So is the tech giant, Apple. In fact, several technology firms choose to be secretive for similar, perfectly justifiable, reasons.

There are also a number of firms whose mission is to protect their clients from organised crime. A good example here is Control Risks. This low-key company helps to resolve crises such as kidnapping and industrial espionage.[3] To do this it employs a wide range of technologists, lawyers, aid workers, investigators, cyber experts, political scientists, soldiers, strategy consultants and intelligence officers. With a mission to use its 'investigative expertise to help resolve conflict', Kroll is another private intelligence agency used by governments and corporations to help gain and leverage hidden information and evidence of poor business practice. Both these organisations are carrying out legitimate activities by necessity away from public scrutiny. And, of course, there have always been those with particular interests who have privately lobbied governments to support a cause or espouse a point of view – and often with positive effect.

Beyond this in recent years we have seen the rise of a number of semi-autonomous organisations that exist at the interface of government and society. In the main these have emerged from within the global aerospace, defence, security or advanced technologies industries. They have an increasingly wide remit although they are often focused on the acquisition of industrial know-how and generating access to leading-edge technology, with a notable growth in associated industrial espionage. With an initial focus on defence and weapons systems, microelectronics and software development, they are also active in industrial chemicals, automotive and, more recently, cybersecurity sectors. Some are part of mainstream companies; some are dedicated security firms; some are formally planned off-shoots or sub-groups of government bodies; many are linked to intelligence and security agencies such as the CIA, NSA, MI5, MI6, KGB / FSB, BND, Mossad, Shin-Bet, Bureau 39 or the Ministry of State Security in China.

Many successful brands have chosen to keep their internal activities and strategy hidden.

Dark Organisations

Secretive organisations are one thing but the growth in the number of smaller organisations whose operations are largely hidden from view, and, quite possibly, regulatory oversight was raised at our workshops. Some are seeking to defend assets; others wish to discover more about their competitors or develop new means of surveillance. Perhaps unsurprisingly these organisations are generally run by those with connections to, or who are previous employees of, the military or intelligence services. Although often small, generally their client base often has access to hefty budgets and comprise governments and large corporations. As a result, these companies are beginning to have a profound effect on the international stage.

Somewhat ambiguously several organisations in and around this space, perhaps aiming to build on their brand identity, have included 'Dark' or 'Black' in as part of their name. For example:

- **Blackwater –** (now renamed Academi and part of the Constellis organisation) is one of several US based private military companies that expanded significantly in Iraq and Afghanistan;[4,5]
- **Black Cube -** an Israeli private intelligence agency;[6] and
- **DarkMatter –** a UAE based firm conducting both defensive and offensive cybersecurity.[7]

Although an aside, this frequently causes confusion not only between each other but also with the use of the word 'dark'. Take, for example, the dark web (the part of the internet not indexed by search engines),[8] dark pools (private forums for trading securities, derivatives, and other financial instruments)[9] and dark companies (publicly listed firms that have stopped filing SEC returns and often leaving shareholders with heavy losses and a stock they know nothing about).[10]

Several organisations in and around this space, perhaps aiming to build on their brand identity, have included 'Dark' or 'Black' in as part of their name.

Organisations of Influence

Over and above all of this, in varied discussions, we have been alerted to a number of organisations with growing influence behind the scenes which are operating beyond normal practice, either on the edge of, or, in some instances, over the line of, what is legal (in some countries) and what society may see as appropriate. For some, their growing influence is causing considerable concern.

From the dialogues we see three types of hidden organisations:

1. **Hiding in plain sight:** These are visible to the public in one area of activity but are undertaking morally questionable activities in another;

2. **Exposed companies:** These have 'crossed a line' or two and are acting outside the bounds of what is generally considered is acceptable; and

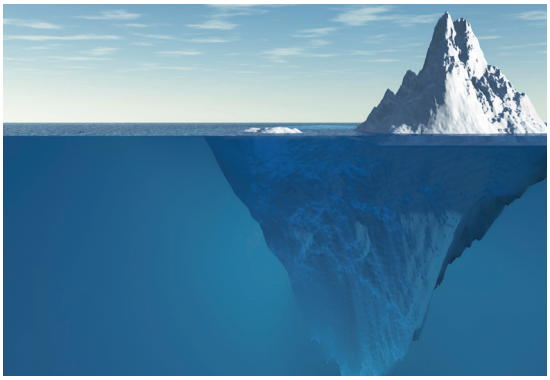
3. **Covert operators:** These are undertaking activities that are illegal in some nations but are supported by others' governments.

Several of those we have heard about operate behind the scenes - beyond public record, but to give a flavour of what is underway, here are some examples that have been identified in the mainstream media:

Hiding in Plain Sight

- **23andme** and **ancestry.com** are both well known for providing low-cost DNA and ancestry services to customers worldwide. However, the profitable part of their business is in reselling access to that data to the pharmaceutical sector and other third parties without recompense to the individual customers. A $300m deal between 23andme and GSK in 2018 is just the start of a broader monetisation of personal health data.[11] In South Africa we were informed that the government has banned sharing of health data with 23andme.

- During a data discussion in Dubai it was revealed that several major **exam boards** have made access to the full data sets of an individual student performance throughout their education a precondition for them to gain their qualifications. Schools are obliged to comply, but parents and students are largely unaware of the data transfer.[12]



- Throughout the Brexit negotiations, financial lobbyists such as **The City UK** were contracted by negotiators on both sides of the table. "While corporate interests sought to shape the future trade deal in their own interests, the public remained in the dark."[13]

- In Iceland, hedge fund, the **Baupost Group,** intentionally bought distressed debt and then went to great lengths to hide it.[14] The firm then profited from the collapse of the Icelandic Banks through a string of shell companies that were difficult to trace.

The issue with these examples is that some companies are taking actions that are at odds with their stated propositions. The public believe one story but in fact companies are generating revenue from another route. In general, those who attended our workshops found this behaviour to be ethically dubious and, in some jurisdictions, it was considered illegal. If this was more widely recognised there may be greater public concern. While not advocating authoritarian government control of corporate activities, some we spoke to suggest that there should be greater up-front transparency around what is going on.

Exposed Companies

- The publication of the 2016 Panama Papers which uncovered the fact that 8% of the world's wealth ($7.6tn) was stashed in tax havens and the revelations about law firm **Mossack Fonseca** was a turning point for many.[15] Although there was some awareness of the complex approaches taken to help the super-rich hide their money few were aware of the scale of the operations. The media coverage brought this into the mainstream and highlighted the extremes of wealth inequality. With a global tax loss of over $200bn including $78bn there was great anticipation of change in how governments close the loopholes – but, as yet, little seems to have had tangible impact.

- **UBiome** is a US firm focused on human microbiome sampling which positioned itself as a "citizen science start-up." Its initial fundraising drew criticism from ethicists regarding both consent issues with respect to direct-to-consumer-testing and the business advisability of launching a biotech start-up with crowdfunding but was given regulatory approval nonetheless.[16] It was only when the FBI investigated UBiome's billing practices that it went into bankruptcy in order to 'reorganise'

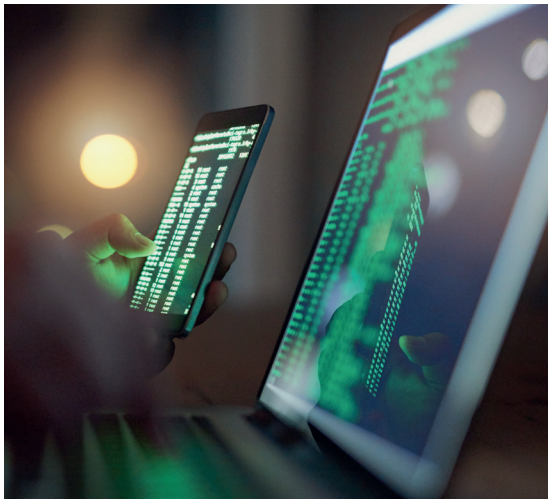
- **Clearview AI** is seen by the New York Times, for one, as "The secretive company that might end privacy as we know it."[17] The AI facial recognition firm has already amassed over 3 billion photos harvested from scraping myriad social media platforms.[18] Its software is already being used by over 600 police forces as well as the FBI to help identify potential criminals. Some see that the company "keeps lying while selling incredibly powerful facial recognition that traffics in regular peoples' sensitive data"[19] Several scholars are raising the alarm. As Woodrow Hartzog, at Harvard's Berkman Klein Centre for Internet and society, sees it, "we've relied on industry efforts to self-police and not embrace such a risky technology, but now those dams are breaking because there is so much money on the table: I don't see a future where we harness the benefits of face recognition technology without the crippling abuse of the surveillance that comes with it."[20] Other privacy experts see this as part of "a larger conversation taking place, both in the United States and abroad, about whether and how the powerful technology should be regulated."[21]

Revelations such as these serve to highlight malpractice that is becoming increasingly impactful. While the Mossack Fronseca case may lead to curtailment of unethical practice in some areas, there is little to suggest there will be a change in direction for Clearview AI which has the support of a growing customer base across different areas of government. Of particular concern for several analysts we spoke to is that these, and a growing number of similar examples, are being exposed because they have tripped up on a side-issue. UBiome was given the regulatory ok for its contentious fundraising approach but pulled up by the FBI for a different issue of billing. With Clearview AI it is academics raising the alarm not government. Oversight that is either absent or severely lacking may well be letting others pass unnoticed.

Covert Operators

- Regularly identified during our discussions has been **Palantir Technologies'** much planned and now accelerating move into healthcare. However, the company's history has raised concerns around its suitability for a role in civilian organisations. Although it's website states that it was "founded on the conviction that it's essential to preserve fundamental principles of privacy and civil liberties while using data" it is closely connected to the NSA and provides surveillance related services to several US government security agencies as well as to more than ten other nations.[22] It also offers a range of supporting software, including Gotham which "aggregates massive amounts of personal data, enabling law enforcement officers to gain a broad understanding of a suspect's life without a warrant."[23] Palantir has had ambitions to enter the healthcare sector and monetise medical data for a while. This year, as part of the US CDC and UK NHS responses to Covid-19 it has been granted wide access to national health data sets without charge and is using its Foundry AI to "enable disparate data to be integrated, cleaned, and harmonised in order to develop the single source of truth that will support decision-making."[24] It is making similar pitches to Germany, Austria, Switzerland and France.[25] Twelve months ago, the UK government was exploring whether it could make $10bn a year by renting access to its aggregated, anonymised health data set. Now it has given Palantir and others full access to the raw data for free and a growing number are duly concerned.[26]

- In the same sector, health platform **K App** has access to 400 million doctor-patient consultations and 1.4 billion lab results. It is one of several AI start-ups with close links to the Israeli military.[27] It has been keen to promote itself as an algorithm-based program to inform patients on the likely conditions people with symptoms like theirs have.[28] Again, privacy and ethics experts are concerned about how the company is using this type of medical data: "This is one of the biggest



hacks of privacy in Israel. We are going to be very sorry for this process in the near future."[29] In response the company's CEO's view is that "in every country, there are things that happen secretly and that's a good thing so long as there is oversight."[30]

- In the world of surveillance, UAE-based **DarkMatter** describes itself as a purely defensive company, but it is alleged to be involved in offensive cybersecurity on behalf of the Emirati government. It is one of several Middle Eastern organisations staffed by ex-NSA employees, endorsed by their previous employer but criticised by others as digital mercenaries.[31] A recent Reuters article on Project Raven, the underlying programme, shared insight into the role former American cyber-spies play in foreign hacking operations.[32] The firm is now under investigation by the FBI for crimes including digital espionage services, involvement in the Jamal Khashoggi murder, and incarceration of foreign dissidents.

- Also, in the Middle East, Israeli firm **NSO** has developed software, Pegasus, that accesses Apple, Amazon, Google and Facebook cloud data and can allegedly also hack Android smartphones and iPhones as well as WhatsApp.[33] Indeed,

WhatsApp has filed US lawsuits claiming that NSO has been 'deeply involved' in hacking its users "by "knowingly" and "wilfully" targeting WhatsApp's systems to disseminate malware."[34] Since being profiled by the FT in 2019, the company has "denied promoting hacking or mass-surveillance tools for cloud services" and "maintained that its software, which is designated by Israel as a weapon, is only sold to responsible governments to help prevent terrorist attacks and crimes." However, as it has now made Pegasus available to other clients, this line may well have been crossed.

- Back in the financial services sector, there are a number of firms operating at the intersections of fields such as crypto-currencies and derivatives. The UK regulator, amongst others, has been trying to impose a ban on crypto-based derivatives for retail investors including those provided by **Kraken Futures**.[35] An FCA study found it is "impossible to reliably value the derivatives contracts linked to them." It also suggested that the market is "driven by speculation," rather than technological or economic developments and was "akin to gambling". The company is however still active in the field and has recently also announced an expansion into Russia.[36]

- Lastly, and taking a wider cross-sector but more customer-focused perspective, the **Society for Trust and Estate Practitioners** (STEP) is a London-based representative body of wealth managers.[37] It has been singled out by a number of government agencies in several countries concerned with tax evasion, money laundering and growing worldwide wealth inequality.[38] Key customers are around 200,000 'ultra-high net-worth' individuals worldwide.[39] Most of them want their investments to be kept private, often in trusts, but concerns are being raised, even by offshore bankers, as to what vehicles their wealth managers are investing their funds in and to what purpose.[40] STEP is involved in dialogue with government agencies such as the HMRC on tax reform but is very much considered to be defending its client's interests.[41]

Although these examples offer different extremes, what connects them is that the lack of transparency means they can operate without supervision. Often this is because the technology being used, whether AI for surveillance or algorithmic investing, is leading-edge and pushing the boundaries of what is possible. Although it may be that some are also migrating into more legitimate areas, this does little to instil trust in their actions. In short, the acceleration of wholesale repurposing of security analytics for civilian applications, such as healthcare or financial services, deserves greater public scrutiny and regulatory control.

As these organisations scale in size and reach, and, as they diversify into more mainstream areas, their impact looks set to grow. Because many have been established by ex-military and government employees seeking to capitalise on their old networks and specialist skills, this is raising concern about the implications this might have for national security.[42] Take for example a warning by hundreds of global researchers of the potential for bad actors (state, private sector, or hacker) to create 'social graphs' using any of the tracing apps that are now widely available in order to spy on citizens' real-world activities.[43]

As these organisations scale in size and reach, and, as they diversify into more mainstream areas, their impact looks set to grow.

Future Impact and Implications

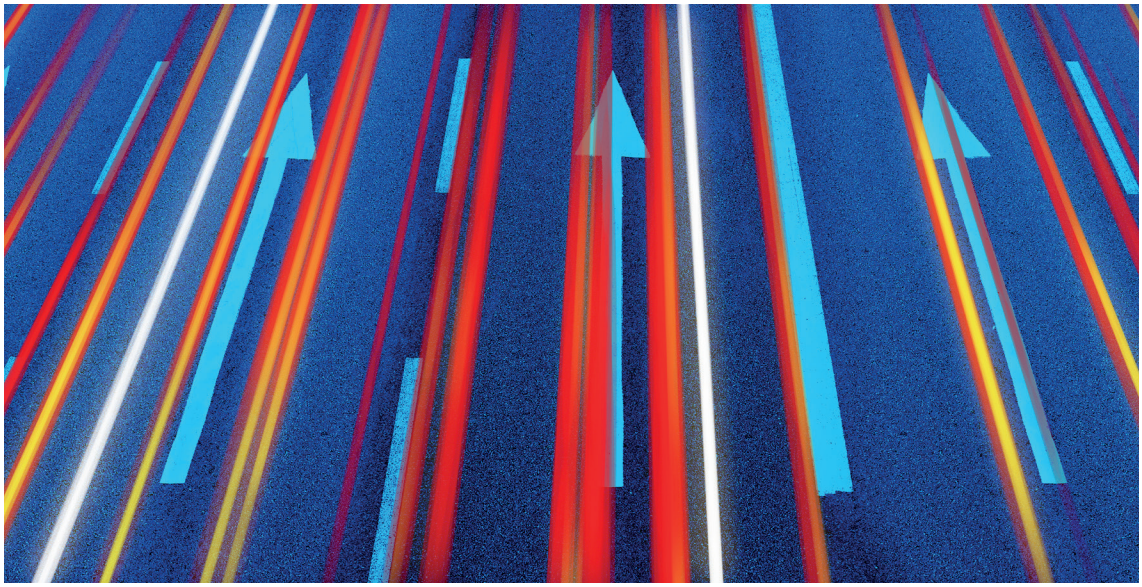
Opacity is not necessarily inevitable. In the corporate world and momentum is building to call hidden actors to account. The UK government, for instance, is adapting the Companies House register to know more about who is setting up, managing and controlling organisations and improve the detection of possible criminal behaviour.[44] More broadly OpenCorporates is one of a number of websites trying to provide better public insight.[45] It uses machine learning to uncover interlinkages "to ensure that everyone knows exactly who they are working with – and working for. To tackle corruption and criminality. To protect our democracy. To create a trusted business environment, we want to work in – and a society we'd all like to live in." This is now the largest open database of companies in the world, covering over 184m companies and 234m corporate officers.

Perhaps the most notable action of all is coming from the Citizen Lab at the University of Toronto.[46] This interdisciplinary group's research includes "investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analysing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities." As well as being prominent in uncovering the activities of NSO and its Pegasus software, the Citizen Lab has recently also focused on the security concerns around 5G technology from Huawei and Google's cooperation with China on the, now terminated, Dragonfly search engine project.[47]

Perhaps the most notable action of all is coming from the Citizen Lab at the University of Toronto.

Leading in 2030

It is clear that public bodies should increasingly tread carefully before they agree partnerships with privately held entities. Without the appropriate levels of regularity involvement, sensitive and confidential personal data can be easily scraped and monetised for commercial purposes and, once the genie is out of the bottle, it may be difficult to backtrack. Initiatives such OpenCorporates and Citizen Labs offer a sign of how the power dynamic, which often seems to be at the behest of the elite, could potentially to be turned on its head. After all, if better data about companies, or even governments, becomes more widely available perhaps it will be possible to start challenging their activities more effectively. This suggests that in the future it may well become a little more difficult for unaccountable organisations to wield their influence away from the public eye.



References

[1] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[2] https://mediacenter.23andme.com/company/about-us/

[3] https://www.controlrisks.com/our-services/resolving-critical-issues-and-crises

[4] https://en.wikipedia.org/wiki/Academi

[5] https://constellis.com/who-we-are/overview

[6] https://en.wikipedia.org/wiki/Black_Cube

[7] https://en.wikipedia.org/wiki/DarkMatter_(Emirati_company)

[8] https://en.wikipedia.org/wiki/Dark_web

[9] https://en.wikipedia.org/wiki/Dark_pool

[10] http://www.nonamestocks.com/p/dark-companies.html

[11] https://www.forbes.com/sites/nicolemartin1/2018/12/05/how-dna-companies-like-ancestry-and-23andme-are-using-your-genetic-data/#3288bbfa6189

[12] https://www.deliveringvaluethroughdata.org

[13] https://corporateeurope.org/en/power-lobbies/2018/10/brexit-trade-deal-finance-lobby-allowed-work-secret

[14] https://www.institutionalinvestor.com/article/b17t99npw9smz1/how-hedge-funds-hide

[15] https://www.theguardian.com/news/2016/apr/08/mossack-fonseca-law-firm-hide-money-panama-papers

[16] https://www.forbes.com/sites/alexknapp/2019/05/01/microbiome-startup-ubiome-cofounders-on-administrative-leave-after reports-of-fbi-raid/#2e5b24b85829

[17] https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

[18] https://www.forbes.com/sites/kateoflahertyuk/2020/01/26/clearview-ais-database-has-amassed-3-billion-photos-this-is-how-if you-want-yours-deleted-you-have-to-opt-out/#6d6202a760aa

[19] https://www.vox.com/recode/2020/2/11/21131991/clearview-ai-facial-recognition-database-law-enforcement

[20] https://cyber.harvard.edu/story/2020-01/secretive-company-might-end-privacy-we-know-it

[21] https://iapp.org/news/a/concerns-around-regulation-of-facial-recognition-technology-on-the-rise/

[22] https://www.forbes.com/sites/thomasbrewster/2020/03/31/palantir-the-20-billion-peter-thiel-backed-big-data-giant-is-providing-a coronavirus-monitoring-tool-to-the-cdc/

[23] https://www.forbes.com/sites/michaelposner/2019/09/12/what-companies-can-learn-from-palantir/#1e22a44216e0

[24] https://healthtech.blog.gov.uk/2020/03/28/the-power-of-data-in-a-pandemic/

[25] https://www.bloomberg.com/news/articles/2020-04-01/palantir-in-talks-with-germany-france-for-virus-fighting-tool

[26] https://www.telegraph.co.uk/technology/2020/05/16/inside-story-cia-backed-palantir-embedded-nhs-socialite-running/

[27] https://www.wsj.com/articles/israel-prepares-to-unleash-ai-on-health-care-11568599261

[28] https://journals.lww.com/md-journal/Fulltext/2019/10180/_A_patient_like_me____An_algorithm_based_program.57.aspx

[29] https://www.wsj.com/articles/israel-prepares-to-unleash-ai-on-health-care-11568599261

[30] https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

[31] https://www.aljazeera.com/news/2019/12/white-house-veterans-helped-uae-build-secret-surveillance-unit-191210195734339.html

[32] https://www.reuters.com/investigates/special-report/usa-spying-raven/

[33] https://www.ft.com/content/95b91412-a946-11e9-b6ee-3cdf3174eb89

[34] https://twitter.com/jsrailton/status/1253502720885108736

[35] https://www.ft.com/content/bfc2759e-9d77-11e9-b8ce-8b459ed04726

[36] https://www.kraken.com/en-us/

[37] https://www.step.org/about-us

[38] https://www.theguardian.com/business/2016/sep/21/how-to-hide-it-inside-secret-world-of-wealth-managers

[39] https://www.capgemini.com/news/world-wealth-report-2019/

[40] https://academic.oup.com/tandt/article-abstract/doi/10.1093/tandt/ttx098/4004853/Review-by-Jersey-Finance-of-Trusts Weapons-of-Mass?redirectedFrom=fulltext

[41] https://www.step.org/sites/default/files/Policy/STEP_Response_7_Nov_2018.pdf

[42] https://drive.google.com/file/d/1uB4LcQHMVP-oLzIlHA9SjKj1uMd3erGu/view

[43] https://drive.google.com/file/d/1OQg2dxPu-x-RZzETlpV3lFa259Nrpk1J/view

[44] https://companieshouse.blog.gov.uk/2019/06/11/how-were-reforming-the-companies-house-register/

[45] https://opencorporates.com

[46] https://citizenlab.ca/about/

[47] https://citizenlab.ca/category/lab-news/mentions/page/2/

FUTURE AGENDA
Open Foresight

The World in 2030

This is one of 50 global foresights from Future Agenda's World in 2030 Open Foresight programme, an initiative which gains and shares views on some of the major issues facing society over the next decade. It is based on multiple expert discussions across all continents and covers a wide range of topics. We do not presume to cover every change that will take place over the next decade however we hope to have identified the key areas of significance. Each foresight provides a comprehensive 10-year view drawn from in-depth expert discussions. All foresights are on https://www.futureagenda.org/the-world-in-2030/

Previous Global Programmes

The World in 2020 was published in 2010 and based on conversations from 50 workshops with experts from 1500 organisations undertaken in 25 countries as part of the first Future Agenda Open Foresight programme. This ground-breaking project has proven to be highly accurate in anticipating future change and the results have been used by multiple companies, universities, NGOs and governments globally. Rising obesity, access not ownership, self-driving cars, drone wars, low cost solar energy, more powerful cities and growing concerns over trust were just some of the 50 foresights generated. For more details: https://www.futureagenda.org/the-world-in-2020/

Five years on, the World in 2025 programme explored 25 topics in 120 workshops hosted by 50 different organisations across 45 locations globally. Engaging the views of over 5000 informed people, the resulting foresights have again proven to be very reliable. Declining air quality, the growing impact of Africa, the changing nature of privacy, the increasing value of data and the consequence of plastics in our oceans are some of the foresights that have already grown in prominence. For more details: https://www.futureagenda.org/the-world-in-2025/

About Future Agenda

Future Agenda is an open source think tank and advisory firm. It runs the world's leading Open Foresight programme, helping organisations to identify emerging opportunities, and make more informed decisions. Future Agenda also supports leading organisations on strategy, growth and innovation.

Please contact us via:
douglas.jones@futureagenda.org

Future Agenda
84 Brook Street
London W1K 5EH
www.futureagenda.org
@futureagenda

Text © Future Agenda 2020
Images © istockimages.com and corporate libraries