G20 INSIGHTS

G20 GERMANY 2017
THINK 20 DIALOGUE

Economy, Employment and Education in the Digital Age

G20 2020

A Step to Implementing the G20 Principles on Artificial Intelligence: Ensuring Data Aggregators and AI Firms Operate in the Interests of Data Subjects

Paul Twomey (Centre for International Governance Innovation (CIGI)),

Kirsten Martin

April 3, 2020 | Last updated: April 6, 2020

This Policy Brief is offered to the Saudi T20 process, as a recommendation to the G20 in 2020.

In the offline world, we have developed safeguards to ensure that those with intimate knowledge of others do not exploit vulnerabilities and weaknesses of individuals through manipulation. Yet, online data aggregators and their related AI firms, with whom we have no relationship (for instance a contract), have more information about our preferences, concerns, and vulnerabilities than our priests, doctors, lawyers, or therapists. We propose that Governments should extend their existing off-line protections and standards against manipulation to also cover these data controllers which presently have the knowledge and proximity of a very intimate relationship without the governance and trust inherent to such relationships in the off-line market. We also propose several steps to protect citizens' autonomy and decrease user deception. The ability of 'data traffickers' and their AI partners to leverage knowledge they have on almost every person on the Internet makes the scale of the public policy and political challenge worthy of Ministers and Heads of Government.

Challenge

A long standing tenet of public policy in both advanced and emerging economies is that where an economic actor is in a position to manipulate a consumer – in a position to exploit the relative vulnerabilities or weaknesses of a person in order to usurp their decision making– society requires their interests to be aligned and punishes acts that are seen as out of alignment of the interests of the person. Individuals in some relationships, for example between priests-parishioners, lawyers-clients, doctors-patients, teachers-students, therapists-patients, etc., are vulnerable to manipulation through the intimate data collected by the dominant actor, and these types of relationships are governed such that the potential manipulator is expected to act in accordance with the interests of the vulnerable party. We regularly govern manipulation that undermines choice, such as when negotiating contracts under duress or undue influence, or when contractors act in bad faith, opportunistically, or unconscionably. The laws in most countries void such contracts.

When manipulation works, the target's decision making is usurped to pursue the interests of the manipulator; and the tactic is never known by the target. Some commentators rightly compare manipulation to coercion (Susser, Roessler, and Nissenbaum 2019). For coercion, a target's interests are overtly overridden by force and the target knows about the threat and coercion. Manipulation, on the other hand, overrides a target's choice subversively. Both seek to overtake the authentic choice of the target and just choose different tactics. In this way, manipulation has the goals of coercion and the deception of fraud. And offline, we regulate manipulation similar to the way we regulate coercion and fraud: to protect consumer choice-as-consent and preserve the autonomy of the individual.

Online actors, such as data aggregators, data brokers, and ad networks, can not only predict what we want and how badly we need it but can also leverage knowledge about when an individual is vulnerable to making decisions in the interest of the firm. Recent advances in hyper-

targeted marketing allows firms to generate leads, tailor search results, place content, and develop advertising based on a detailed picture of their target. Aggregated data on individuals' concerns, dreams, contacts, locations, and behaviors allows marketers to predict what consumers should want and how to best sell to them. It allows firms to predict moods, personality, stress levels, health issues, etc. – and potentially use that information to undermine the decisions of consumers. In fact, Facebook recently offered advertisers the ability to targets teens when they are 'psychologically vulnerable.'

Proposal

All this information asymmetry between users and data aggregators has sky-rocketed in recent years.

The data collection industry is not new. Data brokers like Acxiom and ChoicePoint have been aggregating consumers' addresses, phone numbers, buying habits and more from offline sources and selling them to advertisers and political parties for decades. But the Internet has transformed the space. The scope and intimacy of the data collection and the purposes for which it is sold and used is rarely comprehended by users.

One reason for this is that much of the data is collected in a non-transparent way and mostly in a manner that people would not consider covered by contractual relationships. Many Internet users, at least in developed countries, have some understanding that the search engines and the e-commerce engines collect data on what sites they have visited and that this data is used to help tailor advertising to them. But most have little idea of just how extensive this commercial surveillance is. A recent analysis of the terms and conditions of the big US platforms shows that they collect 490 different types of data on each user (2).

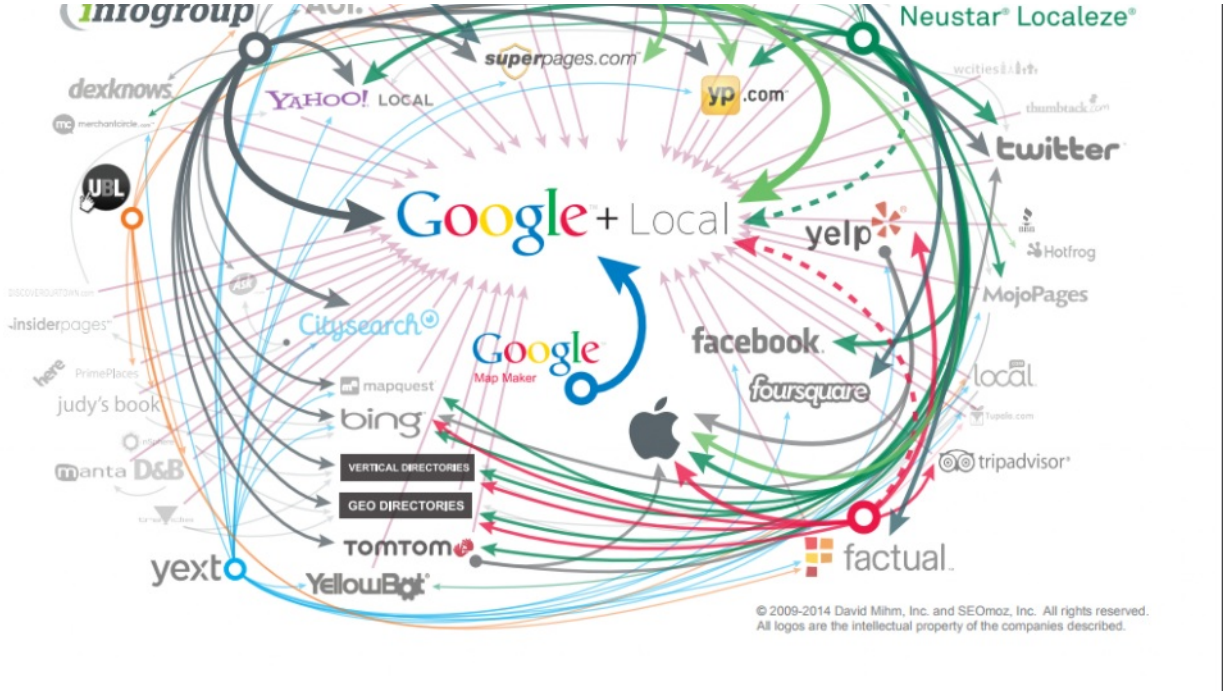
A recent study of 1 million web sites showed that nearly all of them allow third party web trackers and cookies to collect user information to track page usage, purchase amounts, browsing habits, etc. Trackers send personally identifiable information such as user's name, address, and email and spending details. These latter allow the data aggregators to then de-anonymize much of the data they collect (Englehardt and Narayanan 2016, Libert, 2015).

But cookies are only one of the mechanism used to collect data on people. Both little known data aggregators and the big platforms draw huge amounts of information from cell towers, the use of the devices themselves, many of the third party apps running on the user's device, Wi-Fi access, as well as public data sources and third party data brokers.

As the New York Times recently reported:

Every minute of every day, everywhere on the planet, dozens of companies — largely unregulated, little scrutinized — are logging the movements of tens of millions of people with mobile phones and storing the information in gigantic data files. The Times Privacy Project obtained one such file [which] holds more than 50 billion location pings from the phones of more than 12 million Americans as they moved through several major cities… Each piece of information in this file represents the precise location of a single smartphone over a period of several months…It originated from a location data company, one of dozens quietly collecting precise movements using software slipped onto mobile phone apps (4).

An indication of the scale and complexity of the collection and transfer of user data among web sites can be gleaned from the following diagram. Devised by David Mihm, a noted expert on search engine optimization, it shows the data feeds contributing to the US online local search ecosystem (5).



It is data collection networks and markets like these, invisible to the vast majority of the people whose personal data is being collected, which enable Cambridge Analytica (of the 2016 US Presidential election fame) to claim that it holds to have up to five thousand data points on every adult in the US (6).

Initial steps by governments

The questions of the correct governance for Artificial Intelligence and its underlying Big Data have been discussed at national and dispersed international fora for several years. These include efforts by the Council of Europe (7), the Innovation Ministers of the G7 (8), the European Parliament (9) and the OECD (10).

In June 2019, the G20 Trade Ministers and Digital Economy Ministers adopted a set of AI Principles (11) which drew from the OECD's principals and discussion of proposals from G20 engagement groups (12). These principles point to a more human-focused and ethical approach to guiding AI – but they are by necessity broad in tone and lacking in regulatory specifics.

The intimate data collection and transfiguration conducted by many AI systems in recent times mimic the vulnerable relationships offline, yet the safeguards we find in offline relationships have not yet to be put in place. Large AI systems, including the Platforms, accumulate data/knowledge and hence power asymmetries that render consumers/citizens vulnerable to manipulation and exploitation. Furthermore, many of these firms operate without relationships to the targets – indeed many of the data aggregators for AI are completely unknown to the individuals on whom they collect and manipulate vast amounts of data.

This is contrary to several sections of the G20 AI Principles. In particular Section 1.1 ("Stakeholders should proactively engage in responsible stewardship of trustworthy AI in pursuit of beneficial outcomes for people… reducing economic, social, gender and other inequalities."), Section 1.2 (" AI actors should respect the rule of law, human rights and democratic values, throughout the AI system lifecycle. These include freedom, dignity and autonomy, privacy and data protection, non-discrimination and equality, diversity, fairness, social justice, and internationally recognized labor rights.") and Section 1.3 ("AI Actors should commit to transparency and responsible disclosure regarding AI systems… enable those affected by an AI system to understand the outcome; and… those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic.")

Regulating manipulation to protect consumer choice is not novel. What is unique now is that the current incarnation of manipulation online divorces the intimate knowledge of the target and power used to manipulate from a specific, ethically-regulated relationship as we usually find offline. Online we now have a situation where firms, with whom we have no relationship, have more information about our preferences, concerns, and vulnerabilities than our priests, doctors, lawyers, or therapists. In addition, these firms, such as ad networks, data brokers, and

data aggregators, have an ability to reach specific targets due to the hypertargeting mechanisms available online. Yet, we are not privy to who has access to that information when businesses approach us with targeted product suggestions or advertising. These data brokers have the knowledge and proximity of an intimate relationship covering very personal parts of our lives without the governance and trust inherent to such relationships in the market. They clearly fail the transparency, stewardship, non-discrimination, autonomy, and fairness provisions of the G20 Principles.

Current Approach to Regulating Manipulation Online

In the offline world sharing information with a particular market actor, such as a firm or individual, requires trust and other safeguards such as regulation, professional duties, contracts, negotiated alliances, nondisclosure agreements, etc. The point of such instruments is to share information within a (now legally binding) safe environment where the interests of the two actors are forced to be aligned. However, three facets of manipulation by data traffickers (13)– those in a position to covertly exploit the relative vulnerabilities or weaknesses of a person in order to usurp their decision making – strain our current mechanisms governing privacy and data. First, manipulation works by not being disclosed, thus making detection difficult and rendering the market ill-equipped to govern the behavior. Second, the type of manipulation described herein is performed by multiple economic actors including websites/apps, trackers, data aggregators, ad networks, and customer facing websites luring in the target. Third, data traffickers – who collect, aggregate, and sell consumer data – are the engine of manipulation of online consumers yet have no interaction, contract, agreement with individuals.

These three facets – manipulation is deceptive, shared between actors, and not visible by individuals – render the current mechanisms ineffective in governing the behavior or the actors. For example, GDPR is strained when attempting to limit a 'legitimate use' of data traffickers or data brokers who are looking to market products and services based on intimate knowledge. An individual has a right to the restriction of processing of information only when there are no legitimate grounds of the data controller. This makes GDPR fall short because legitimate interests can be broadly construed to include product placements and ads. And the manipulation of individuals has not been identified (yet) as diminishing a human right of freedom and autonomy. One fix is to more clearly link manipulation to individual autonomy, which would be seen as a human right that could trump even the legitimate interests of data traffickers.

A first step forward – Policy Goals

In general, the danger comes from using intimate knowledge about an individual and hyper-targeting to then manipulate them. The combination of individualized data and individualized targeting needs to be governed or limited:

1. **Protect Autonomy**. Manipulation is only possible because a market actor, here it is data brokers, has intimate knowledge of individuals as to what renders a target vulnerable in their decision making. The goal of governance would be to limit the use of intimate knowledge by making certain types of intimate knowledge either illegal or heavily governed. The combination of intimate knowledge with hyper-targeting of individuals should be more closely regulated than blanket targeting based on age and gender. Explicitly recognize individual autonomy, defined as the ability of individuals to be the authentic authors of their own decisions, as a legal right in order to protect individuals from manipulation done in the name of "legitimate interests" within the AI Principles.
2. **Expand Definitions of Intimate Knowledge.** One step would be to explicitly include inferences made about individuals as sensitive information within such existing regulations as GDPR (Wachter and Mittelstadt 2019). Sandra Wachter and Brent Mittelstadt have recently called on rights of access, notification, and correction for not only the data being collected but the possible inferences drawn from the data about individuals. These inferences would be considered intimate knowledge of individuals that could be used to manipulate them (e.g., whether someone is depressed or not based on their online activity). The inferences made by data traffickers based on a mosaic of information about individuals can constitute intimate knowledge as to who is vulnerable and when. Current regulatory approaches only include collected data as protected rather than the inferences drawn about individuals based on that data.
3. **Force Shared Responsibility.** Make customer-facing firms responsible for who they partner with to track users or to target users. Customer-facing websites and apps should be responsible for who is given access to their users' data – whether by sale or whether given access by placing trackers and beacons on their site. Third parties include all trackers, beacons, and third parties who purchase data or access to their users. Websites and apps would then be held responsible for whether they partner with firms that abide by GDPR standards, AI Principles, or new standards of care in the U.S. Holding customer facing firms responsible for how their partners (third party trackers) gather and use their users' data would be similar to holding a hospital responsible for how the patient is cared for by their contractors in the hospital or holding a car company responsible for a third party app in the car that then tracked your

movements. This would force the customer-facing firm, with whom the individual has some influence, to make sure their users' interests are being respected (16). The shift would be to have customer-facing firms be held responsible for how their partners (ad networks and media) treat their users.

4. **Expand the Definition of "Sold".** Make sure all regulations include beacons and tracking companies in the any requirement to notify if user data is 'sold'.

5. **Create a Fiduciary Duty for Data Brokers** There is a profound, yet relatively easy to implement, step to address this manipulation. G20 and other governments could make their AI Principles practical by extending the regulatory requirements they have on doctors, teachers, lawyers, government agencies and others who collect and act on the intimate data of individuals to also apply to data aggregators and their related AI implementations. *Any actor who collects intimate data about an individual should be required to act on, share, or sell this data consistent with the interests of the person.* This would force the alignment of interests between the target/consumer/user and the firm in the position to manipulate. Without any market pressures, data brokers who hold intimate knowledge of individuals, would need to be held to a fiduciary-like standard of care for how their data would be used.(Balkin 2015) This would mean data brokers would need to be responsible for how their products and services were used to possibly undermine the interests of the individuals.

6. **Add Oversight**. Add a GAAP-like governance structure over data traffickers and ad networks to ensure individualized data is not used to manipulate. With these economic actors well outside any market pressures, there are few pressures on the firms to align their actions with users' interests. A third step would be to make data traffickers abide by GAAP-like regulations. Recently McGeveran called for GAAP-like approach for data security, where companies would be held to a standard defined for all firm similar to the use of GAAP standards for accounting. However, the same concept should be applied to those who hold user data as to how they protect the data when profiting from it (17). Audits could also be used in order to ensure data traffickers, who control and profit from intimate knowledge of individuals, are abiding by their standards. This would add a cost to those who traffic in customer vulnerabilities and provide a third party to verify that those holding intimate user data act in a way that is in the individuals' interests and protect firms from capitalizing on their vulnerabilities. A GAAP-line governance structure could be flexible enough to understand the market needs while still being responsive to protect individual rights and concerns.

7. **Decrease Deception.** Finally, manipulation works because the tactic is hidden from the target. The goal of governance would be to *make the basis of manipulation open to the target and others.*In other words, make the type of intimate knowledge used in targeting obvious and public. This could mean a notice (e.g., this ad was placed because the ad network believes you are diabetic) or this could mean a registry when hyper-targeting is used to allow others to analyze how and why individuals are being targeted. Registering would be particularly important for political advertising so that researchers and regulators can identify the basis for hyper-targeting. It should not be sufficient for an AI/data aggregator just to say "I am collecting all this information in the interests of the user to see tailored advertising." That is equivalent to a doctor saying "I collect all this data about a patient's health to ensure that the patient only knows the prescription I give the patient." Patients have to give permission for and are entitled to know what data is collected (indeed in many countries patients formally own their health data), what tests have been conducted and their results, what the diagnosis is – and they are entitled to a second opinion on the data. Similar sorts of transparency and accountability offline should apply online. In other areas, where a lawyer or realtor or financial advisor, has intimate knowledge and a conflict of interest (where they could profit in a way that is detrimental to their client), they must disclose their conflict and the basis for their conflict.

In the offline world, we have stressed the importance of clear relationships between people and those who have intimate information asymmetries over them. And we have developed safeguards to ensure that those gaining positions of power do not exploit vulnerabilities and weaknesses of individuals. The issues posed by vast data collection and hyper-targeted marketing and/or service delivery are a product of the global expanse of the Internet, social media and AI platforms. Furthermore, the ability of 'data traffickers' and their AI partners to leverage knowledge they have on almost every person on the Internet makes the scale of the public policy and political challenge worthy of Ministers and Heads of Government. As the growing "tech backlash" shows, there is political mobilization among citizens across the world for change. The innovation of this "apply the offline world rules to the online players" approach is that it does not require governments to educate or force citizens to change behaviors or desires. It puts the ethical and regulatory onus on the firms involved and holds them accountable.

---

(6) See "MPs grill data boss on election influence", 27 February 2018 http://www.bbc.com/news/technology-43211896

(7)https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of- aut/1680796d10

(8) https://g7.gc.ca/en/g7-presidency/themes/preparing-jobs-future/g7-ministerial-meeting/chairs- summary/annex-b/

(9) Directorate-General for Parliamentary Research Services (European Parliament), A governance framework for algorithmic accountability and transparency see at

(10)https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf
https://www.oecd.org/going-digital/ai/principles/

(11) See Annex to G20 Ministerial Statement on Trade and Digital Economy at https://www.mofa.go.jp/files/000486596.pdf

(12) For instance, see Paul Twomey. "Building on the Hamburg Statement and the G20 Roadmap for Digitalization: Toward a G20 framework for artificial intelligence in the workplace." At https://www.g20-insights.org/policy_briefs/building-on-the-hamburg-statement-and-the-g20-roadmap-for-digitalization-towards-a-g20-framework-for-artificial-intelligence-in-the-workplace/

(13) Lauren Scholz first used the term data traffickers, rather than data brokers, to describe firms that remain hidden yet traffic in such consumer data (Scholz 2019).

(16) It is ironic that currently data traffickers can sell data to bad actors but they just can't have their data stolen by those same bad actors.

(17) McGeveran calls for a GAAP like approach for data security. Here we would have the same idea for data protection. Where standards are set and others must be certified to abide by them (McGeveran 2018).

References

1. Balkin, Jack M. 2015. "Information Fiduciaries and the First Amendment." UCDL Rev. 49: 1183. Englehardt, Steven, and Arvind Narayanan. 2016. "Online Tracking: A 1-Million-Site Measurement and Analysis."
   More Information
2. McGeveran, William. 2018. "The Duty of Data Security." Minn. L. Rev. 103: 1135.
3. Scholz, Lauren Henry. 2019. "Privacy Remedies." Indiana Law Journal.
   More Information
4. Susser, Daniel, Beate Roessler, and Helen Nissenbaum. 2019. "Technology, Autonomy, and Manipulation." Internet Policy Review 8 (2).
5. Wachter, Sandra, and Brent Mittelstadt. 2019. "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI." Columbia Business Law Review.

Existing Initiatives & Analysis