ETHICAL CHALLENGES FOR DATA GATHERING INDUSTRIES

Paul Twomey Ph.D.

Co-Founder, Stash.global

Former CEO of Internet Corporation for Assigned Names and Numbers (ICANN)

Prepared for the Fifth Consultation Meeting of the Dublin Process on

An Ethical Compass for the Digital Age: Ethics in International Business and Finance

Centesimus Annus Pro Pontifice (CAPP) Foundation

Fordham University, New York, March 15-17 , 2018

I Introduction

I want to join with others in congratulating Professor Enderle on his thoughtful paper. My discussion paper aims to illustrate the challenges of the explosion of data collection and the shift in human experience being determined by the operation of algorithms. In doing that, I will make draw on the points raised by Professor Enderle, particularly as they relate to the preferential option for the poor as part of this benchmark for the purpose of an economic system.

The perspective of this paper is one of a practitioner. It comes from my experience as a promoter of the Internet economy, a coordinator of Internet protocols and trying to protect businesses and individuals from cyber threats. But it also comes from my public policy experience of helping the transition of political economies to a digital age. And unfortunately, what I have to say is that I am increasingly alarmed about where that societal journey is heading.

Further, society has a real need for the Church to be active here - to hear an informed voice from the biggest single global institution dedicated to the ethical and spiritual. The Church needs to recognize that the poor in the 21st century are the ignorant, the naive and the exploited in a data world as much as the cash poor. She needs to show a preference and support for those poor She needs to be a voice for the many. She needs to inject thousands of years of careful ethical thinking into a policy discussion which now takes place mainly in a bubble of very computer literate Technorati.

The Church needs to loudly proclaim and its spiritual and human-centric view of progress into these debates to leaven the dominant message of technological utopianism.

This paper's title is about the ethical challenges for the data gathering industries. What we need to realise is that we are rocketing to an international economy where nearly every industry will be a data gathering and processing industry. So, the challenges here are going to be universal. Let me discuss these in parts. Firstly, the vast amount of data being collected and how it is being obtained. Secondly, perhaps more importantly, the role and effect of the algorithms into which this data is being poured. Finally, let me make some observations on the urgent challenges this presents to the Church.

II. The Data Challenge

Let us explore how the data collection has changed over the last 20 years.

Data Collection

Data collection is now a big business. But I would argue that most citizens/consumers and church and political leaders have no real understanding just how big and dynamic it is. The McKinsey Global Institute Data stated six years ago that data collection and processing was a $300 billion-a-year industry and employed 3 million people in the United States alone.[1] It has increased at double digit growth rates since then and is accelerating.

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 mobile internet/smart phone revolution has particularly helped drive the growth in data and the personal intimacy of that data. Much of the new data generated is user-generated data. From the beginning of history up to 2003, humanity created about 5 exabytes of information. Now the world creates 2.5 exabytes of data per day. Every digital interaction throws up information which can be used to analyse and predict human behavior. Speaking to this in 2010, Eric Schmidt, then CEO of Google, said "People aren't ready for the technology revolution that's going to happen to them"[2]. I would argue that most still have little idea of how that revolution has taken place around them.

---

[1] https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_exec_summary.ashx

[2] No anonymity on future web says Google CEO, http://www.thinq.co.uk/2010/8/5/no-anonymity-future-web-says-google-ceo/

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.

The search engines place cookies on user's computers to track the sites the IP address of the user, browser configuration, date and time, search content, and the links to sites a user visits. Google's cookie lasts for thirty years and if a user deletes the cookie it is immediately replaced every time the user enters a google domain (even if that it is not to search). Search engine and other main internet services' cookies enable the tracking to continue across all the users' devices. But this is far the extent of tracking of users.

A recent study of 1 million web sites showed that nearly all of them are infected by third party web trackers and cookies which collect user information, delivering user data to others than the owner of the web site including Google, Facebook, and others to track page usage, purchase amounts, browsing habits, etc. Some trackers even 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. In specifics the Annenberg School for Communication at the University of Pennsylvania found that:

> Nearly 9 in 10 websites leak user data to parties of which the user is likely unaware; more than 6 in 10 websites spawn third- party cookies; and more than 8 in 10 websites load Javascript code from external parties onto users' computers. Sites that leak user data contact an average of nine external domains, indicating that users may be tracked by multiple entities in tandem. By tracing the unintended disclosure of personal browsing histories on the Web, it is revealed that a handful of U.S. companies receive the vast bulk of user data.[3]

In response to some users concerns, all major Web browsers now allow a message to be sent as part of the user's connection request saying that the user does not want to be tracked. But DNT has no enforcement process. "Investigation of the policies of the top 10 corporations with tracking elements reveals that 9 of them do not respect the DNT header. The *only company* in the top 10 to respect the DNT header is Twitter."[4]

For the stated objective of improved search results or more appropriately targeted advertising, the Internet platforms (Google, Facebook, Amazon, YouTube, Instagram, Apple, Twitter, Reddit, etc.) also combine their data searches to other platforms and have moved away from a policy of only seeking anonymized data to now actively seeking to de-anonymize data and collate all according to user identity. Google for instance retrieves use data of from adsense cookies deployed with sites carrying Google ads and collects server log information, registration and email content information from Gmail accounts.

---

[3] Timothy Libert, "Exposing the invisible web: An analysis of third-party http requests on 1 million websites," *International Journal of Communication*, vol. 9, 2015 pp 3544–3561, p. 3544

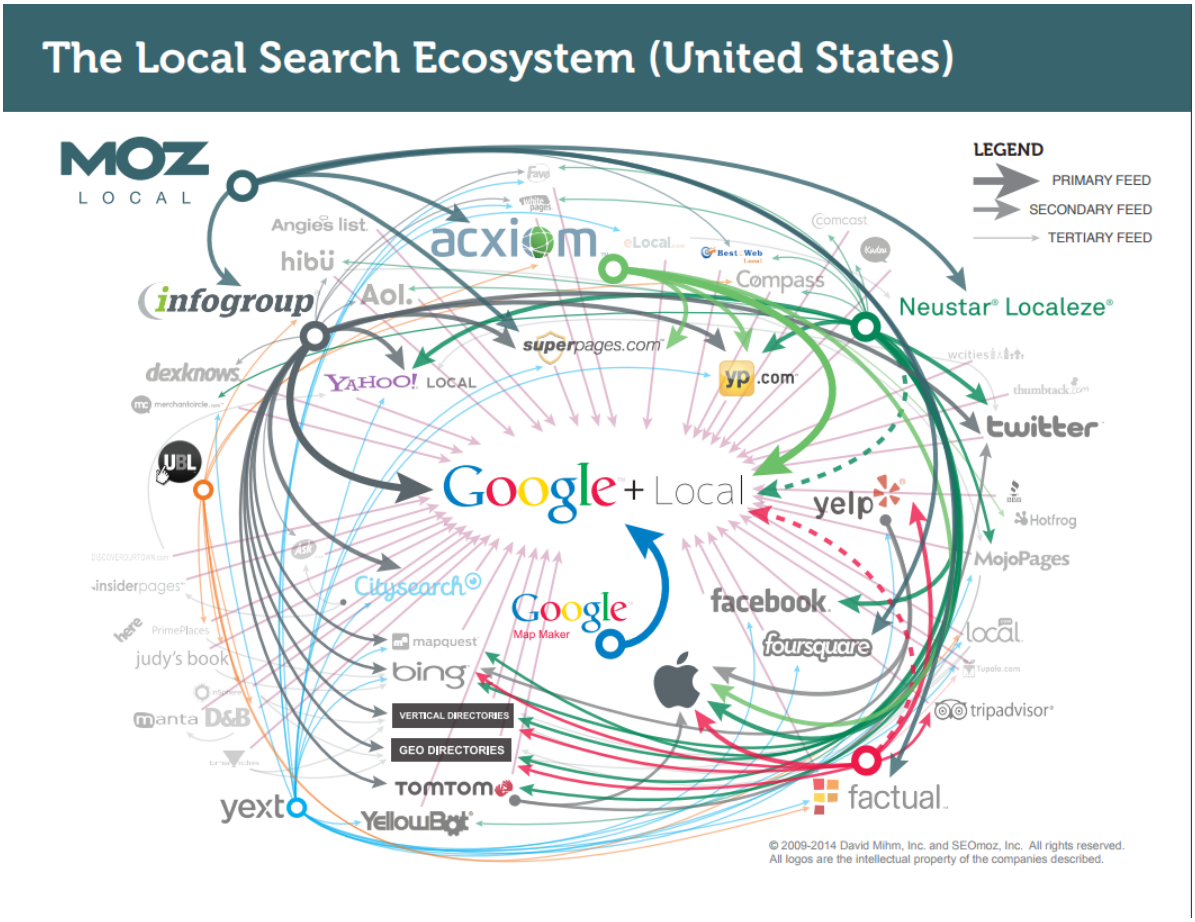
[4] Ibid, p. 3533

Indeed, this determination to collect as much data as possible has now developed a culture in Google which Eric Schmidt recently described as going up to the creepy line. Responding to a question in a conference, Schmidt responded "The Google policy on a lot of things is to get right up to the creepy line and not cross it…. With your permission you give us more information about you, about your friends, and we can improve the quality of our searches...We don't need you to type at all. We know where you are. We know where you've been. We can more or less now what you're thinking about."[5]

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.[6]

[5] https://www.huffingtonpost.com/2010/10/04/eric-schmidt-google-creepy_n_748915.html

[6] https://whitespark.ca/blog/understanding-2017-u-s-local-search-ecosystem/



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.[7]

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

Data Inaccuracy

In addition to the problems of data collection over-reach, there is the related challenge of inaccurate data being collected. Studies have shown that the inaccuracy levels of the data held on individuals by the traditional data aggregators Acxiom and ChoicePoint can be between 18 and 35%.[8]

The web trackers claim to collect accurate user actions and technical data but more sophisticated privacy-oriented users can use cookie blockers and clearing of caches to try to avoid such comprehensive collection. But three problems arise from this:

1. As Libert notes: "Although these add-ons do, indeed, offer a significant degree of protection, they also place the burden on users and highlight the blame-the-victim mentality at the core of the issue."[9]
2. The mere practice of cookie churn may still make it possible to track the individual. Other researchers have concluded "that by applying host- tracking results with other identifiers, service providers may still be able to identify a large fraction (88%) of the "one-time", churned new cookie IDs as corresponding to users who return to the service." "Such patterns can become a distinctive feature that makes tracking easier, despite the user's intention of remaining anonymous."[10]

---

[8] Deborah Pierce and Linda Ackerman: "Data Aggregators: A Study of Data Quality and Responsiveness" for privacyactivism.org, May 19, 2005, https://web.archive.org/web/20070319220412/http:/www.privacyactivism.org/docs/DataAggregatorsStudy.html

[9] Libert, Op.Cit., p. 3557

[10] Ting-Fang Yen, Yinglian Xie, Fang Yu, Roger Peng Yu, and Martın Abadi, "Host Fingerprinting and Tracking on the Web: Privacy and Security Implications", **The 19th Annual Network and Distributed System Security**

3. Further, the fact that a user tries to minimize the amount of data being collected by a data aggregator does not stop the fact that the data aggregator has internal data processing and 3rd party commercial relationships which are reliant on the data being inputted. Just because the input data is scant does not mean that the internal or third-party algorithms are still not run concerning the user. Hence the privacy-aware user may be contributing to effectively false negative data errors in these algorithms.

Ethical Challenges of the Present Data Aggregation Model

Nearly all online data collectors will say that their policies on data collection are stated in their privacy policies and terms of use – and hence, users have agreed to them.

The bottom line is that this line fails the basic courtroom oath. It may be the truth (although for many deployed third-party web trackers this is not clear) but it is not the whole truth. Much of the language is obscure and hidden in voluminous terms of service which the sites know the vast majority of users will not read, nor understand if they do.[11] What the sites don't say upfront is the truth about their business model: In return for your using our service for free (or even paid) we sell your data directly or indirectly to advertisers and other data aggregators – and here is

---

Symposium (NDSS) 2012, The Internet Society. https://www.microsoft.com/en-us/research/publication/host-fingerprinting-and-tracking-on-the-webprivacy-and-security-implications/

[11] From www.Google.com it takes 3-4 clicks to get to a description of the data Google collects and why and brief description of its cookies. For Facebook and Instagram it is 2 clicks. For YouTube, Pinterest and Twitter it is only one click. But none of the sites promote this information – it is definitely placed among the small print. Considering this is the effective price the user is paying for the service, one would expect "this is what you are paying" to be presented clearly.

exactly what sort and how much of that data we collect and here are all the sites from which we collect it. For the overwhelming history of commerce an offer was clear – I sell you this following service or good for the following price in legal tender. Now online vendors promote only free services and impose an asymmetric model on the consumer: the companies have ways of monetizing individual's data but the users don't. They have effectively turned their users into the product they sell.

For many the terms of use could be seen as unconscionable and potentially void.[12] They are often so long and impenetrable as to be not understandable by the user. Further, many (especially new users to the Internet in developing countries) do not realise that the "free to use" model has one side understanding that the currency for cementing this contract is the right to collect as much data as it can from and about the user using technical skills and tools incomprehensible to most users and from online places the user does not associate with the particular Internet company. This is far from a fair or equal relationship and it exploits the innocent and the naive. Furthermore, the pervasive market power of the Internet platforms means that for a person wanting to participate in modern life (in which connection to the Internet is key), there is no realistic way that a user can refuse the terms of use. The terms of use (and their related comprehensive data collection processes) are a form of extortion. They are not an

---

12 "The *unconscionability* defense is concerned with the fairness of both the process of contract formation and the substantive terms of the contract. When the terms of a contract are oppressive or when the bargaining process or resulting terms shock the conscience of the court, the court may strike down the contract as unconscionable.

A court will look at a number of factors in determining if a contract is unconscionable. If there is a gross inequality of bargaining power, so the weaker party to the contract has no meaningful choice as to the terms, and the resulting contract is unreasonably favorable to the stronger party, there may be a valid claim of unconscionability. A court will also look at whether one party is uneducated or illiterate, whether that party had the opportunity to ask questions or consult an attorney, and whether the price of the goods or services under the contract is excessive. " http://smallbusiness.findlaw.com/business-contracts-forms/will-your-contract-be-enforced-under-the-law.html

expression of a realistic free choice. Perhaps the most pernicious aspect of this unrestricted commercial surveillance is that companies collect data on users with whom they have no commercial relationship. I do not use Facebook and do not have any contractual agreement with Facebook. But all across the web, Facebook's web trackers seek to collect data on my use, including personally identified detailed, e-commerce transaction details, and send it back to Facebook. In Australia at least, this seems to me to be formally a breach of the Telecommunications (Interception and Access) Act 1979 (Commonwealth) which provides that only approved law enforcement and intelligence agencies can conduct surveillance of individuals' communications.[13] But the American, and especially northern Californian, origins and culture of the Internet platforms has resulted in their building business models based on the ambiguity in US law as to who has the right to surveille the individual. The topological (rather than geographical) nature of the Internet produces large scale network effects to successful first movers. Hence companies successful in the US when it was the major internet market have transferred that success swiftly to a global Internet market – and brought their business practices with them.

One of the impacts of this early mover advantage is that the vast amount of information being collected from websites used by users around the world is flowing to US companies. Only one indication of this process is to look at what proportion local websites are in the top 25 websites visited by users in a particular country. Researchers reported in 2013 the following:[14]

---

[13] For instance, third party cookies recording user names, purchases and transaction details from a website's e-commerce pages would appear to infringe section 172 "No disclosure of the contents or substance of a communication" of the legislation. https://www.legislation.gov.au/Details/C2017C00308

[14] Claude Castelluccia, Stéphane Grumbach, Lukasz Olejnik. "Data Harvesting 2.0: from the Visible to the Invisible Web", The Twelfth Workshop on the Economics of Information Security, Jun 2013,

Country	National ratio	Foreign Sites
US	100%	No foreign site
China	92%	Only foreign site: Google
Russia	68%	Mostly American sites
Japan	36%	Mostly American sites
South Korea	24%	Half American half Chinese
France	36%	Only American sites
Nigeria	24%	Mostly American sites

The data collected by third party web trackers shows a similar pattern. The search engine data splits between US and Chinese services.

This is an amazing collection of the personal data of the world's Internet users by a group of mostly Silicon Valley followed by Chinese Companies. For users in the developing world, often the understanding of the data collection and transfer is not well understood. Recently at a conference I witnessed a senior official from an African country point out how much her citizens used the US platforms but had little understanding about the data collection and monetization process. She went on to say: "I expect you in the future to compensate our naive citizens for the personal data you are collecting about them."

International policy makers, working from within appropriately slower processes, are beginning to react to these business models. The European Unions' new General Data Protection Regulation goes some way to requiring data processors to tell European residents what data is

Washington, DC, United States. 2013. <hal-00832784> https://hal.inria.fr/hal-00832784/document

being held on them and to correct it if asked to. The GDPR requires "a statement or clear affirmative action" that signals agreement of transferring personal data. It also requires that if the data has not been obtained directly from the data subject, the data controller must outline:

- From which source the personal data originates.
- The existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

As the GDPR comes into effect this year, it will be interesting to see the extent the online data aggregators feel their business model needs to change.

A related area of policy being increasingly questioned is the efficacy of the various national systems of competition policy to address global platform businesses. Competition policy and its related area of consumer protection are key instruments for driving both innovation/new business generation and employment growth.

Recent debate in the United States indicates the importance of identifying optimal principles. A summary of that debate includes:

> When access to certain search engines or social networks is an essential part of participating in contemporary life it may be that these companies should be treated as a natural monopoly, much like a water system, or a railroad. Former top White House adviser Steve Bannon has argued that they should and hence be regulated.[15] The US

[15] https://theintercept.com/2017/07/27/steve-bannon-wants-facebook-and-google-regulated-like-utilities/

Democratic Party's "Better Deal" policy statement also supports stronger competition enforcement, including in the communications sector, without setting specific new methods.[16]

US data indicates that Google gets about 77 percent of U.S. search advertising revenue. Google and Facebook Inc. together control about 56 percent of the mobile ad market. Amazon takes about 70 percent of all e-book sales and 30 percent of all U.S. e-commerce. Facebook's share of mobile social media traffic, including the company's WhatsApp, Messenger, and Instagram units, at 75 percent.[17] Economists such as David Autor, Peter Orszag, Jason Furman, and some in the Chicago School are arguing that this level of market concentration is one of the culprits behind some of the U.S. economy's most persistent ailments - the decline of workers' share of national income, the rise of inequality, the decrease in business startups, the dearth of job creation, and the fall in research and development spending. They are arguing that the companies with market power should be broken up. They point to the innovation benefits of the break up of Ma Bell.

This degree of market concentration is not limited to the US. In China, Alibaba, Biadu and Tencent account for a combined 72 percent of the country's mobile ad revenue.[18]

A third line of thought comes from Albert Wenger, a partner at Union Square Ventures. He argues that the fundamental source of monopoly power in the digital world is network

---

[16] http://www.democraticleader.gov/wp-content/uploads/2017/07/A-Better-Deal-on-Competition-and-Costs.pdf
[17] https://www.bloomberg.com/news/articles/2017-07-20/should-america-s-tech-giants-be-broken-up
[18] http://www.scmp.com/tech/china-tech/article/2076802/alibaba-baidu-tencent-dominate-chinas-red-hot-digital-advertising

> effects arising from the control of data. His proposal is to shift computational power and ownership of the data to network participants.[19]

In the mix of this debate I would add that the present data aggregation model seeks to circumvent one of the key principles of economics: that price is a statement of truth. Price is an indication of how much it takes to produce a product and how much a customer is willing to pay for the benefits of the product. Where consumers are only offered "free" products but are not fully aware of the personal data "price" they are continually paying, nor have any way of calculating the real financial value of this personal data, then the pricing principal is subverted. Such asymmetry in markets also diminishes the reach of the present anti-trust laws, especially those which assume that the primary test is financial harm to the consumer.

Even *The Economist* newspaper has moved to the conclusion that anti-trust laws need to be revamped to overcome the combined effects of massive data collection, the maximising returns effect of network businesses and the data pricing asymmetry with consumers. In a recent leader it stated:

> A radical rethink is required—and as the outlines of a new approach start to become apparent, two ideas stand out.
>
> The first is that antitrust authorities need to move from the industrial era into the 21st century. When considering a merger, for example, they have traditionally used size to determine when to intervene. They now need to take into account the extent of firms'

[19] http://continuations.com/post/163405066045/attention-on-digital-monopolies

data assets when assessing the impact of deals. The purchase price could also be a signal that an incumbent is buying a nascent threat. On these measures, Facebook's willingness to pay so much for WhatsApp, which had no revenue to speak of, would have raised red flags. Trustbusters must also become more data-savvy in their analysis of market dynamics, for example by using simulations to hunt for algorithms colluding over prices or to determine how best to promote competition.

The second principle is to loosen the grip that providers of online services have over data and give more control to those who supply them. More transparency would help: companies could be forced to reveal to consumers what information they hold and how much money they make from it. Governments could encourage the emergence of new services by opening up more of their own data vaults or managing crucial parts of the data economy as public infrastructure, as India does with its digital-identity system, Aadhaar. They could also mandate the sharing of certain kinds of data, with users' consent—an approach Europe is taking in financial services by requiring banks to make customers' data accessible to third parties.

Rebooting antitrust for the information age will not be easy. It will entail new risks: more data sharing, for instance, could threaten privacy. But if governments don't want a data economy dominated by a few giants, they will need to act soon.[20]

[20] "The world's most valuable resource is no longer oil, but data", **The Economist**, May 6th 2017

II Role and Effect of Algorithms

With the rise of populist politics in the democracies, there has been much discussion of the impact of free trade and automation has had on manufacturing workers in countries like the United States. The technological impact on the 21st Century workplace, however, is not limited to labor replacement and geographical shifting because of mechanization and evolving global supply chains. One of its most important impacts is on what data is collected, for what purported purpose, how it is collected analyzed, how the output data is further marketed and collated and analyzed – all of this without transparency to the worker, customer or even management. This is the world of Artificial Intelligence colliding with civil liberties and our existing systems for regulatory/legal and media/civil society oversight.

Increasingly complex and opaque algorithms are driving applications that influence key parts of users' lives, as well as the networks themselves. Via these algorithms, corporations decide what content receives priority and what is ignored. Claiming intellectual property protection, corporate owners often ensure that algorithms are immune from public scrutiny, transparency and accountability – even when they are at the same time demanding more transparent access to government collected data to help fuel their algorithms. This determination to maintain private control over the algorithms which define our online "public square" means that companies like Facebook, Twitter and Reddit struggle to reassure the community about how they can constrain the activities of state actors and others who can game their algorithms.

But this is not just a story about "fake news". This is about how fit for purpose are the millions of algorithms in at the heart of the software which increasingly drive every aspect of our lives.

The reality is that code is written by humans and its complexity can accentuate the flaws humans inevitably bring to any task.

As Airbnb says[21], bias in the writing of algorithms is inevitable. It can have chilling effects on individual rights, choices, the application of worker and consumer protections and democracy. Algorithms are not neutral: they incorporate built-in values and serve business models that may lead to unintended biases, discrimination or economic harm[22]. Compounding this problem is the fact that algorithms are often written by relatively inexperienced programmers, who may not have a correct picture of the entire application, or a broad experience of a complex world. The dependency of the workplace on algorithms imparts tremendous power to those who write them, and they may not even be aware of this power, or the potential harm that an incorrectly coded algorithm may have. Because the complex market of interacting algorithms continues to evolve, it's also possible, and likely, that existing algorithms that may have been very innocuous yesterday will have significant impact tomorrow.

But intellectual property and sometimes even cybersecurity are rewarded by a lack of transparency. Innovation generally, including in algorithms, is a value which should be encouraged. How are these competing values to be balanced?[23]

---

[21] https://airbnb.design/anotherlens/

[22] For instance, media reports have pointed out clear racial bias resulting from reliance on sentencing algorithms used by many US courts. https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html

[23] One possibility is to make algorithmic verifiability rather than full algorithmic transparency an element of oversight in the digital economy. This algorithmic verifiability would require companies to disclose information allowing the effect of their algorithms to be independently assessed, but not the actual code driving the algorithm. This is explored in some degree by the Report of the Global Commission for Internet Governance https://www.ourinternet.org/report

The ethical debate about the purpose and power of algorithms is nascent, yet the need for it is urgent. The explosion of algorithmic privately held business models is affecting nearly every aspect of life. To give it a popular culture perspective, it is the reality behind the common joke "there is an app for that".

Some of the questions we need to ask to preserve a human-focused evolution are:

- How to identify bias in algorithm production and methods to uncover it and counter it. Especially in areas where algorithms determine the choices available to recruiters, work place management, citizens seeking work, impacts on ability to have collective representation in a "platform/gig economy etc.
- What is the appropriate prisms from which to view the ethics of algorithmic decision making, including the distinction between individual rights and collective aims or constraints? As the new Berlin-based watchdog AlgorthmWatch states "existing ethical and legal criteria are not suitable (or, at least, are inadequate) when considering algorithms generally. They lead to a conceptual blurring with regard to issues such as privacy and discrimination, when information that could potentially be misused to discriminate illegitimately is declared private… Given that the issue of ethics always focuses on action and responsibility for this action, however, it is inevitably dependent on structural and situational contextualization. The rules that apply to the state or to a government, for example, can hardly be applied to citizens as individuals. While this

differentiation is standard practice in the realms of ethics and constitutionalism, it has so far been lacking in the debate about automation."[24]

- How to balance the innovation of content industries and delivery across a global Internet, while still protecting and promoting national and community content and culture online. More broadly the balance between the benefits of Globalization and the sense that nations and sub-national communities need strong domestic cultures and cultural expression to maintain their sovereignty and sense of identity. Globalization cannot just be Americanization.
- The fit for purpose of algorithms and their impact on existing consumer protection, competition and civil rights/liberties. How can citizens have confidence that competition or consumer protection or non-discrimination norms are being followed by major companies and government if actions are taken by interacting sets of algorithms written by unaccountable and inexperienced software developers? What transparency or accountability to purpose should be required of the algorithms which are increasingly defining what we are and are not allowed to do?
- What should be the appropriate human controls and 'rules of war' which should be embedded in the fast-growing area of Lethal Autonomous Weapons Systems?
- How to ensure the centrality of human control over the evolution of a networked society/economy – especially concerns about a widespread, networked Artificial Intelligence environment being beyond concerted human control.

---

[24] Lorena Jaume-Palasí and Matthias Spielkamp, "Ethics and algorithmic processes for decision making and decision support", AlgorithmWatch Working Paper No. 2 p2 https://algorithmwatch.org/en/ethics-and-algorithmic-processes-for-decision-making-and-decision-support/

Some groups and companies[25] have begun to respond to these questions but the acceleration of automated decision making into every aspect of life calls for an urgent and open debate on the ethical framework for 21st century citizens' experience of political, administrative, commercial and social reality.

IV Response required of the Church.

As a practitioner in this fast moving environment, regularly meeting with others and debating these issues while designing and developing applications, let me argue that there is an urgent need for the Church to be more informed and certainly more engaged in the ethical issues facing the Information Society.

---

[25] Microsoft has recently laid out its present thinking about the ethical deployment of Artificial Intelligence (AI). Calling for AI to put humans at the centre, Microsoft proposes six principles:

- Fairness: When AI systems make decisions about medical treatment or employment, for example, they should make the same recommendations for everyone with similar symptoms or qualifications. To ensure fairness, we must understand how bias can affect AI systems.
- Reliability: AI systems must be designed to operate within clear parameters and undergo rigorous testing to ensure that they respond safely to unanticipated situations and do not evolve in ways that are inconsistent with original expectations. People should play a critical role in making decisions about how and when AI systems are deployed.
- Privacy and security: Like other cloud technologies, AI systems must comply with privacy laws that regulate data collection, use and storage, and ensure that personal information is used in accordance with privacy standards and protected from theft.
- Inclusiveness: AI solutions must address a broad range of human needs and experiences through inclusive design practices that anticipate potential barriers in products or environments that can unintentionally exclude people.
- Transparency: As AI increasingly impacts people's lives, we must provide contextual information about how AI systems operate so that people understand how decisions are made and can more easily identify potential bias, errors and unintended outcomes.
- Accountability: People who design and deploy AI systems must be accountable for how their systems operate. Accountability norms for AI should draw on the experience and practices of other areas, such as healthcare and privacy, and be observed both during system design and in an ongoing manner as systems operate in the world.

https://msblob.blob.core.windows.net/ncmedia/2018/02/The-Future-Computed_2.8.18.pdf

Since *Rerum novarum* in 1891, the Church's social teaching has been dedicated to understanding and critiquing the social issues of the day. As Professor Enderle has pointed out, this teaching about the obligations of capital and labour has of recent decades also been moulded by the preferential option for the poor. The rapid transformation of the world to an information economy, tied together by a topological network which does not recognize geographic boundaries, is arguably the most significant change in the working and social lives of billions of people since the onset of the industrial revolution. It is a change which has brought great benefits and individual empowerment; but also the collection and analysis of huge amounts of personal data in ways that are poorly recognized by the many new Internet users in the developing world as well as many users in the developed economies.

The Church needs to recognize that the poor in the 21st century are the ignorant, the naive and the exploited in a data world as much as the cash poor. She needs to be a voice for the many. She needs to inject thousands of years of careful ethical thinking into a policy discussion which now takes place mainly in a bubble of engineering-focused Technorati. In a world where Facebook, Google and their co-frères have billions of users, there is no other large international institution recognized by billions of people for its ethical voice in the modern world. Online is a world where scale and brand matter. The Church has an opportunity and an obligation to bring its voice and status to bear on some of the most foundational issues for the next century.

The Church needs to loudly proclaim and its spiritual and human-centric view of progress into these debates to leaven the dominant message of technological utopianism. When Eric Schmidt

can say "I actually think most people don't want Google to answer their questions, they want Google to tell them what they should be doing next" one can see the need for an ethical and Gospel-focused injection into the world of data and algorithms.[26]

[26] Holman W. Jenkins Jr. "Google and the Search for the Future" **Wall Street Journal,** August 14, 2010 https://www.wsj.com/articles/SB10001424052748704901104575423294099527212