IRIE
International Review of Information Ethics Vol. 32 (11/2022)

Author: Alfredo M. Ronchi

Is ethics evaporating in the cyber era? Part 2: Feeling framed

Abstract:

In continuation to the Part 1 published in this volume, this part discusses the oversupply of information and approaches the concerning rights we are alienating to enjoy digital technology. Instead of using the Internet as space for free exchange of ideas, it is being used as a tool for supervision, management, and control. There is an increasing merger of artificial intelligence and machine learning in any sector for analysing, optimizing, and even framing humans. Our digital "buddies" take note of our everyday life, our itinerary, our health parameters, our messages and our content. Big data centres, computer farms are the new "caveau" (Bank Vault) full of "our" data.

Keywords: Appification, Artificial Intelligence, Digital Technology, Ethics, Info-besity, Machine Learning, Privacy

Agenda:

Oversupply of information (info-obesity) 2

Goodbye privacy 2

Artificial Intelligence (AI) and Machine Learning (ML) 3

Machine Learning.....4

To conclude: Do you not feel framed? 6

Authors:

Prof Alfredo M. Ronchi

- Head of S2D2 JRC Politecnico di Milano, Email: alfredo.ronchi@polimi.it

ISSN 1614-1687

Oversupply of information (info-obesity)

We are flooded by emails, online news, video clips, chats, unsolicited advertisements and more. If we simply want to clean up our device every day, we must invest a significant portion of our time that could otherwise be spent for scouting reliable information (Bohn 2009). One of the potential drawbacks due to info-obesity is the devaluation and loss of trust in professional media, together with the deep technological intrusion, affecting our daily life. It is paradoxical that the cyber devices are framing us more than they support us. Some evident outcomes of this feeling are the "right to disconnect[1]" (controversial reform of French labour law by the Labour Minister Myriam El Khomri back in May 2016) and the "right to obsolescence" or the "right to be forgotten" (according to Viktor Mayer-Schönberger, the author of "Delete: The Virtue of Forgetting in the Digital Age"[2]).

The "right to disconnect" is self-explanatory and states the abolition of non-stop "digital slavery". The "right to be forgotten" refers to the intellectual property from the "continental[3]" standpoint that, in addition to the "economic" rights, identifies, even more relevant, some moral rights, like paternity, adaptation, modification and to be able to "withdraw". The author has the moral right to "withdraw" his work of art from the private or public domain. If we keep the similarity in the field of personal data, we must claim the right to withdraw them from the "digital universe". This right is usually termed "right to obsolescence" or the "right to be forgotten". Viktor Mayer-Schönberger traces the important role that forgetting has played throughout human history. He examines the technology that is facilitating the end of forgetting: digitization, cheap storage and easy retrieval, global access, multiple search engines, big data analytics, machine learning, infinite replications of information, etc.

Goodbye privacy

The concept of "data" as it relates to people's everyday life is still evolving (Burrus 2014). We inherited the concept of copyright and we, more recently, faced the concept of privacy (Merriam Webster). Cyber technology contributed in relevant mode to the sudden and initially invisible shift to "goodbye privacy" and blurring of ethical principles. Cyberspace is not a black hole, a kind of "outer space" or a no man's land, where personal data is not subjected to humans' material desires and malicious behaviours. The APPification process boosted the dissemination of personal data, and the more technology we use, the more visible we become. We live in a world in which there are already countless sensors and smart objects around us all the time.

The car we drive, the phone in our pocket, our wristwatch, the clothes we wear, are smart and connected; then the concept of "private" becomes far more ephemeral. IoT will add a lot to our lives, but this will cost us a significant part of our privacy. We may say "we have nothing to hide", but others may maliciously use our personal data (Ronchi 2018). Our personal information is now shared among several companies. We will never be sure that it will disappear from the online database. This takes us to another relevant point, the concept of data ownership, which refers to the copyright. If the data are ours, we can delete them at our will, isn't it?

Copyright and copyleft are two sides of the same coin. They both refer to the most relevant aspect of intellectual property. Traditionally, copyright and copyleft have been regarded as absolute opposites: the former being concerned with the strict protection of authors' rights, the latter ensuring the free circulation of ideas. Indeed, a commonly held belief about copyleft is that it begins where the boundaries of copyright end, spreading over

[1] loi n 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels https://www.theguardian.com/money/2016/dec/31/french-workers-win-legal-right-to-avoid-checking-work-email-out-of-hours, last accessed January 2019.

[2] Mayer-Schönberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009.

[3] In the domain of intellectual property rights "continental" is the European (ethic and moral driven) approach instead of the Anglo-Saxon one (mainly revenue based)

a no man's land of more or less illegal exploitation. Recently, the European Commission boosted the concept of Open Science as a powerful tool to significantly improve research achievements. The running Horizon Europe Framework opted for the Open Science approach "by design". Hence, all the EU funded projects must publish their scientific outcomes and ensure long term access to them through specific data repositories.

Both copyright and privacy are derived from the concept of data ownership. For example, we take a picture of a landscape and add our name as the author/owner on it and publish it on our web page. If someone else downloads our picture, crops the author's name, and posts it on his/her website, it's a copyright infringement. Nowadays open data is one of the most popular buzzwords. If a public authority will release different sets of "open data", apparently anonymised (UK Government), the combined use of them may lead to identifying our personal behaviour, which is regarded as a form of privacy invasion or perhaps violation (Darrow 2016).

Historically speaking, the idea of even owning information is relatively new[4]. The earliest copyright laws, which granted the creator of artworks, among the other rights, exclusive rights to duplication and distribution of said work, first appeared in the early 18th Century. Nevertheless, it would still be hundreds of years before the concept of "data", as we understand it, even began to develop (Darrow 2016). As observed in the Part 1, ownership of data (My Data) is not yet a well-defined legal concept, though the recent introduction of the GDPR is a significant step forward (EU Regulation). We all agree about privacy and intellectual property infringement, but personal data even if belonging to the same "galaxy" are not properly identified and protected. If this represents the state of the art, in general, it might not always be the case. Individual nations and international organizations are attempting to establish rules governing who can collect what data and what they're allowed to do with it. Germany has a legal concept known as "*informationelle Selbstbestimmung*" or informational self-determination. What does informational self-determination mean? An individual has the right to decide for himself or herself what information can be used by whom and for what. If we focus on cyber-rights, we must prioritise the right to safety, security, and ownership. Information system hacking can compromise both safety and security (data, smart home, smart cities, smart mobility, etc.). Cyber-attacks and Hybrid Threats depict a new scenario in the 21st century. Digital identity thefts create additional challenges.

Artificial Intelligence (AI) and Machine Learning (ML)

Artificial Intelligence (AI), cutting edge technology, in the eighties was depicted by the press as a dangerous shift of humans towards technological slavery. Unfortunately, when AI was adopted initially to the Japanese stock exchange, due to some "bugs" in the system the market crashed. However, later the concrete application of AI was addressed to make, among the others, washing machines and camcorders smarter. The traditional domain of Artificial Intelligence generated along its path some specific domains of application - making our software, home appliances, accessories, and cars - more "intelligent". This evolution was accompanied by the usual philosophical debate on "Can machine think?" The reference study in this regard is indubitably due to Alan Mathison Turing, mathematician, philosopher, cryptographer and more. In his article "Computing machinery and intelligence"[5] the first paragraph "The Imitation Game" of his article "Computing machinery and intelligence"[6] starts with - "I propose to consider the question, "Can machines think?" This begins with the definitions of the terms "machine" and "think." He explains his vision on "thinking machines" providing a more sophisticated definition and revolutionary insight on future technologies. Now AI is back on stage with a completely different impact on society.

[4] My data belongs to me. http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-dis cussion-personal-data-virtualisation-society-wsis10-review

[5] A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460., https://www.csee.umbc.edu/courses/471/papers/turing.pdf last access March 2022.

[6] A. M. Turing (1950) Computing Machinery and Intelligence. Mind 49: 433-460., https://www.csee.umbc.edu/courses/471/papers/turing.pdf last access March 2022.

In the era of open and big data, AI allows extremely large data sets to be analysed computationally to reveal patterns in any kind of datasets (social, political, medical, business, etc), which are used to inform "managers" and enhance decision-making. We used to identify two different branches of AI: "General" also known as "strong AI" and "Narrow" also known as "weak AI".

On the side of strong AI, we find a broad-spectrum artificial intelligence designed to face a wide range of problems "imitating" the human brain. On the side of weak AI, we find vertical solutions based on a well-defined domain of knowledge, for instance, expert systems or automatic car driving systems. They are designed to deal with a specific domain of knowledge, characterised by well-defined rules and situations. They can be further designed to implement machine learning. Additional everyday examples are intelligent personal assistants, chatbots, SIRI, ALEXA, GOOGLE Assistant, and Mercedes Benz and Volkswagen onboard assistants.

Narrow AI (NAI) - Narrow AI is a collection of technologies that rely on algorithms and programmatic responses to simulate intelligence, generally with a focus on a specific task. In the past, this was the branch of AI addressed to create expert systems, a software application designed to solve specific problems providing the rationale of the outcomes. For instance, it is narrow AI when we use a voice-recognition system, like Amazon's Alexa, to turn on the lights. Alexa may sound smart, but it doesn't have any advanced understanding of language and can't determine the meaning behind the words we speak. The program simply listens for key sounds in our speech and, when it detects them, follows its programming to execute certain actions. To users, this can seem surprisingly intelligent — and voice recognition is far from a simple computing task — but there is no actual "thinking" going on behind the scenes. Non-player characters (NPCs) in games are another good example of NAI. While they take human-like action, they are simply following a pre-programmed series of actions designed to mimic how a human would play the game.

General Artificial Intelligence (GAI) - GAI, in contrast, is intended to think on its own. The goal of GAI research is to engineer AI that learns in a manner that matches or surpasses human intelligence. GAI is designed to learn and adapt, to make a decision tomorrow that is better than the one it made today. None of this is easy, which is why most examples of AI we will encounter today are the narrow form. GAI is a new, complex, and varied category with numerous sub-branches, most of which are still research topics in a lab. Modern AI systems focus on solving specific tasks, such as optimization, recommendation, or prediction systems, and don't learn broad concepts generally, as a human would.

Machine Learning

Machine learning (ML) is an interesting subset of AI that is providing inspiring solutions to complex problems. A typical field of application is the one non-approachable with algorithms and explicit programming. The basic principle is to analyse data and identify patterns that can suggest a way to extrapolate a significant result. The typical taxonomy of ML is at the top level subdivided into supervised learning and unsupervised learning.

- Supervised learning: A system "tutor" feeds the application with a set of inputs and expected outputs to train the system that has to identify a general rule that maps inputs and outputs. Of course, this is a possible option when this "rule" is not identifiable by the software programmer. So, without a specific algorithm it is not doable.
- Semi-supervised learning: The system receives only incomplete training. There is no complete set of outputs related to the list of inputs.
- Reinforcement learning: The key feature of this approach consists in a dynamic environment that provides a score (positive or negative) regarding the strategy to be followed to reach the requested output. Thanks to this assessment cycle, we can say that the system learns and provides better solutions as much as it runs[7].

[7] Bishop, C. M. (2006), Pattern Recognition and Machine Learning, ISBN 0-387-31073-8, Springer

- Unsupervised learning: The learning algorithm is completely independent, it does not receive any information about the outputs or any score, and it must identify by itself the structure of the input and discover potentially hidden patterns or identify a potential goal, thanks to feature learning.

Supervised machine learning algorithms and models use labelled datasets, beginning with an understanding of how the data are classified, whereas unsupervised models use unlabelled datasets and figure out features and patterns from the data without explicit instructions or pre-existing categorizations. Reinforcement learning, on the other hand, takes a more iterative approach. Instead of being trained with a single data set, the system learns through trial and error and receives feedback from data analysis. With faster and bigger computation capabilities, ML capabilities have advanced to deep learning, a specific kind of ML that applies algorithms called "artificial neural networks" composed of decision nodes to train ML systems more accurately for supervised, unsupervised and reinforcement learning tasks. Deep learning approaches are becoming more widespread but come with high computation costs and are often harder for humans to interpret because the decision nodes are "hidden" and not exposed to the developer. On the contrary, traditional NAI algorithms are used to provide the rationale behind the outcomes step by step. Nonetheless, deep learning offers a wealth of possibilities, and already has promising applications for image recognition, self-driving cars, fraud news detection and more.

To better clarify the role of ML we can consider, among the others, two typical tasks it can perform:

- Classification: Inputs are divided into two or more classes (labelled). The system must produce a model that assigns additional random inputs to one or more of these classes[8]. As we will see in the following taxonomy, this process is usually performed in a supervised manner. The classes are defined a priori. A typical example of classification tasks performed by ML is spam filtering; the two classes are, of course, "spam" and "not spam". The learning process will increasingly add filters to better perform the classification.
- Clustering: The task is to divide a set of inputs into groups (unlabelled); it looks like the classification tasks but this time the groups are not known beforehand. This is typically an unsupervised task.

Let us leave this side of the technology to face another relevant one, how to deal with responsibilities in case of accidents that directly involve AI or ML?

If we refer to air control, probably one of the closest sectors, the choice is usually between technical problems and human factors. Many times, the final verdict is a mix of several causes that altogether lead to a disaster. Accordingly, with the reports, 70% of aviation accidents can be attributed to human error. Why? Because humans are active players inside the systems, and they are the only components that during emergencies can adapt and adjust resources to try to cope with unexpected events. Of course, these responsibilities are not only to pilots in charge, but they are also related to organisational failures, conditions of the operators (physical and mental state), physical and technological failures and finally human errors.

We increasingly hear of car driver assistance technologies or even autopilot. In case of law infringement or accident, who is considered as responsible, the "driver", the car builder, the software company, or all of them? As usual, in risk analysis, in addition to risks due to our behaviour or decisions, we have risks that do not fall under our control. We must consider that even the "road environment" is part of the system, horizontal and vertical signals. Timely updates of maps and road works are an integral part of the package. Some lane control systems are cheated by multiple lane lines due to the continuing visibility of the old lines. Some accidents involving "intelligent" cars and even humans that have happened and the responsibilities are yet to be assigned. Last but not least, the ethical aspect will merge with intelligent algorithms.

[8] In case of more classes it is termed "multi-label classification".

To conclude: Do you not feel framed?

However, Google, Facebook, Twitter, Apple, Microsoft, Amazon, and any of the other hundreds of companies that can and do collect data about us can use "our" data for all kinds of amazing things. In the "APPification" era there are almost no limits to data collection and reuse. "Someone" knows exactly where you are now and where you have been. APPs may collect your medical data, fitness program, your expenses or collect and analyse your contacts, your photos or video clips, access your smartphone camera and microphone (Ronchi 2018). What about the push message asking to provide details about your activities yesterday evening, something that your digital "buddy" was unable to trace? Your bank will suggest, accordingly with some intelligent algorithms the average monthly expenses due to profiles matching with yours and send an alert if you are exceeding the limit. Computer vision will enable your smartphone to identify every single person in a group you photographed and video analysis plus 3D real-time modelling enable intelligent optimisation algorithms to improve human performances, wearable sensors and IoT completes the schema.

Do we not feel framed by such an "intelligent" environment? Social and communication media complete the panorama adding a "private depth" to the general fresco, ad-hoc defined tweets or posts may collect and analyse users' feedback to guide or anticipate citizens 'actions and feelings'. In recent times, crowd data collection, open data, and big data, more or less anonymised, have provided the big framework to collect all the different tiles. Online malls and delivery platforms offer, in addition, to analysing your browsing, the opportunity to save a "wish list" to better focus on the market trends. So, again don't we feel framed?

References

Bohn, Roger E., & Short, James E. (2009), How Much Information? 2009, Global Information Industry, Center University of California, San Diego.

Burrus, Daniel (2014), Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/

Darrow, Barb (2016), The Question of Who Owns the Data Is About to Get a Lot Trickier, Fortune, http://fortune.com/2016/04/06/who-owns-the-data/

Mayer-Schönberger, Victor (2009), Delete: the virtue of forgetting in the digital age. Princeton University Press. ISBN-13: 978-0691138619

Merriam Webster (nd), Ethic, http://www.merriam-webster.com/dictionary/ethic

My data belongs to me (nd), http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review

Protection of personal data in EU (nd), http://ec.europa.eu/justice/data-protection/

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Ronchi A.M., (2018), Cybertechnology: Use, abuse and misuse, ISBN 978-5-91515-070-X, UNESCO IFAP Interregional Library Cooperation Centre – Moscow, Moscow, Russian Federation

UK Government (nd), UK government service design manual: open data. https://www.gov.uk/service-manual/technology/open-data.html