

# Algorithms: Law and Regulations

**Philip Treleaven**, University College London

**Jeremy Barnett**, St. Paul's Chambers and Gough Square Chambers London

**Adriano Koshiyama**, University College London

*The legal status of AI and algorithms continues to be debated. Resume-sifting algorithms exhibit unethical, discriminatory, and illegal behavior; crime-sentencing algorithms are unable to justify their decisions; and autonomous vehicles' predictive analytics software will make life and death decisions.*

**R**ecently, Elon Musk stated AI is an “existential threat to humanity” and needs urgent regulation “before it is too late.”<sup>1</sup> In a similar vein, pioneering computer scientist Ben Shneiderman, in his 2017 Turing Lecture on algorithmic accountability, called for a “national algorithm safety board.”<sup>2</sup>

Over the years, there have been proposals to regulate robots and algorithms. These include science fiction writer Isaac Asimov's famous 1942 proposal “Three Laws of Robotics”; the South Korean Government's proposal in 2007 of a Robot Ethics Charter; a 2011 proposal from the U.K. Engineering and Physical Sciences

Research Council of five ethical “principles for designers, builders, and users of robots”; and the Association for Computing Machinery's seven principles for algorithmic transparency and accountability, published in 2017. The IEEE has begun developing a new standard to explicitly address ethical issues and the values of potential future users.<sup>3</sup> This new standard, IEEE P7000, aims to establish a process model by which engineers and technologists can address ethical considerations throughout the various stages of system initiation, analysis, and design.<sup>4</sup>

In this era of ubiquitous, pervasive algorithms, AI and soon blockchain smart contracts, three axes of discussion are emerging: when-to regulation, where-to jurisdiction, and how-to technology.

Digital Object Identifier 10.1109/MC.2018.2888774  
Date of publication: 22 March 2019

Opinion is polarized on regulation. For instance, 1) code is law, i.e., this is progress, don't stop innovation; 2) owner responsibility, i.e., the company is legally responsible, therefore, just apply existing laws; 3) code of conduct, i.e., self-regulation by programmers and companies works best; 4) sectorial regulations, i.e., leave regulation to specific sectors, such as financial regulators; 5) algorithm safety board, i.e., a special national authority is required because of the pervasiveness of algorithms; and 6) AI is considered harmful, i.e., ban AI algorithms at least in certain critical applications. One axis covers increasingly sophisticated algorithms and the other covers increasing levels of regulation, as shown in Figure 1.

With regard to jurisdiction, Europe may decide to heavily regulate AI and algorithms, the United States may use existing legislation, and China may do nothing. This will only encourage "regulatory arbitrage," as companies (and innovation) move to the most conducive environment.

Finally, we have technology. What technology options are available for

algorithms to be regulated and proved legal? For example, many machine-learning algorithms 1) are "black boxes" and, thus, are unable to explain their decision-making process, a growing legal requirement in consumer applications; 2) use proprietary Internet Protocol, which the developers are unwilling to divulge; 3) evolve as they learn by assimilating new data that change their behavior; and 4) operate increasingly in algorithm-algorithm ecosystems where future behavior is dynamic and unpredictable. As previously discussed, this article is intended to foster debate concerning the legal status of "intelligent" algorithms in the computer science community.

## CURRENT DEBATE

In this section, we review the debate on the role of algorithms and their regulation and oversight. While many authors are raising public awareness, we can mention Cathy O'Neil's *Weapons of Math Destruction*<sup>5</sup> and Frank Pasquale's *The Black Box Society*,<sup>6</sup> two popular science books that reveal decisions made by opaque, nonauditable,

and unaccountable models in our lives, ranging from obtaining car insurance, loans, and so on to reinforcing discrimination by unethically designed decisions. Nick Bostrom's *Superintelligence*<sup>7</sup> addresses the threat that an unaligned "superintelligent" machine (reachable this century) can cast upon us. All of these authors provide persuasive arguments about the imminent threat that a lack of oversight, standards, and ethics pose to humanity.

It total, there are three areas, ethics, legal, and technology, being investigated by academia and industry with the goal of alleviating or avoiding the impact of intelligence algorithms.

## Ethics

There is a growing body of literature about the implications that unethically designed intelligent algorithms can have for society. Mittelstadt et al.<sup>8</sup> reveal the gap between those that design, operate, and use these algorithms and society at large and then propose a debate across six types of concerns prompted by algorithmic decision making. Making an algorithm

	Self-Regulation	Apply Current Law	Sector Regulation	Algorithm Safety Board	Ban AI
<b>Chatbots</b>	Moderated by Possible Reputational Damage	Existing Laws Cover Slander and so on	Appropriate for Existing Regulators	ASB Advice for Specialist Systems	Not Appropriate
<b>Robo Advisors</b>	Suitable for Informal Consumer Advice	Existing Laws Cover Discrimination, Ethical Behavior, and so on	Appropriate for Existing Regulators	ASB Certification for Critical Systems	Certain "Black-Box" Systems Banned
<b>Control Algorithms</b>	Suitable for Algorithms in Consumer Devices	Existing Laws Cover Contracts, Agencies, and so on	Appropriate for Existing Regulators	ASB for Safety-Critical Infrastructure	Safety-Critical "Black-Box" Systems Banned
<b>Self-Drive Vehicles</b>	Not Appropriate	Existing Laws Cover Driving and Operation	Existing Laws Need Updating	Legislation for "Algorithm Driving Test"	Totally Autonomous Vehicles Banned
<b>Intelligent Robots</b>	Not Appropriate	Existing Health and Laws Appropriate	Existing Laws Need Updating	Specialist Algorithm Certification Required	"Killer" Robots Largely Outlawed

**FIGURE 1.** AI and algorithms—when and how to regulate.

fair is a paramount goal, and meaningful advances<sup>9</sup> have been made to remove (and understand) any bias that is embedded in its decision-making process. A great deal of work in this sense can be found in the annual events of fairness, accountability, and transparency in machine learning ([www.fatml.org](http://www.fatml.org)).

This area is increasingly gaining institutional support; examples include the Future of Life Institute, the Future of Humanity Institute, the Center for the Study of Existential Risk, and the newest, the Ada Lovelace Institute in the United Kingdom, with a US\$7 million backing from the Nuffield Foundation. These organizations are devoted to building a shared understanding of the ethical questions raised by the application of data and intelligent algorithms as well as to developing an evidential basis for how these technologies affect society and different groups within it.

### Legal

Debate on the legal aspects of automated decision making focuses on regulating the data rather than the algorithm component. The landmark legislation in Europe is the General Data Protection Regulation (GDPR),<sup>10</sup> a major E.U. regulation that provides rights to individuals pertaining to their data usage and storage. It remains to be seen whether the United States and China will follow suit. Although the GDPR covers some parts of the algorithm component—such as the “right to explanation” of all automated decisions—Wachter et al.<sup>11</sup> raise several reasons to doubt both the legal existence and feasibility of such a right.

In a recent paper, Tutt<sup>12</sup> argues that U.S. criminal and tort regulatory systems will prove no match for the difficult regulatory puzzles that algorithms

pose. He proposes a finite difference approximation (FDA) for algorithms to serve as an expert regulator that develops guidance, standards, and expertise in partnership with industry to strike a balance between innovation and safety. An FDA for algorithms could draw knowledge from financial services regulation because stress testing, capital/margin requirements, risk management, circuit breaking, and so on are tools and practices already tested, implemented, and regulated.

### Technology

The technology debate is mostly led by think tanks and the industry. Noteworthy is the research from the Machine Intelligence Research Institute,<sup>13</sup> AI safety units of Google<sup>14,15</sup>, and OpenAI ([openai.com/](http://openai.com/)) backed by Elon Musk, Microsoft, and many other entrepreneurs and tech companies.

Public figures, such as the late Stephen Hawking,<sup>16</sup> have also voiced AI safety concerns. Hawking called for a de-escalation of the IT arms race and demanded companies mitigate the risks of these systems being used against humanity. Research institutions and professional associations are now creating blueprints for studies that promote beneficial AI.<sup>4,17</sup>

Overall, the debate in each of these areas is far from a consensus. Action has been taken concerning “data” (e.g., the GDPR and other EU data protection laws), but we have yet to see concrete actions on the algorithms side. Any standards, protocols, and design aspects that emerge for algorithms are likely to focus on the performance, behavior, and “explainability” of intelligent algorithms.

For completeness, we now summarize four core algorithm technologies: AI, blockchain, the IoT, and big data (behavioral/predictive) analytics.

These four technologies are intimately linked, i.e., AI provides the algorithms, blockchain provides the data storage and processing infrastructure, the IoT provides the data, and big data (behavioral/predictive) provides the analysis.

## ALGORITHM TECHNOLOGIES AND ECOSYSTEMS

There are two broad classes of algorithm, which can be termed *static algorithms* (i.e., traditional programs that perform a fixed sequence of actions) and *dynamic algorithms* (i.e., those that embody machine learning and evolve). It is these latter intelligent algorithms that present complex technical challenges for testing and verification, which will underpin regulation.

### AI technologies

AI provides computers with the ability to make decisions and learn without explicit programming. There are two main branches:

- ▶ *Knowledge-based systems*: These are computer programs that reason, and knowledge is explicitly represented as ontologies or rules rather than implicitly via code. For example, in rule-based systems, where the knowledge base contains the domain knowledge coded in the form of IF-THEN or IF-THEN-ELSE rules. Rule-based systems can explain their decision making.
- ▶ *Machine learning*: These are programs that have the ability to learn without explicit programming and can change when exposed to new data. For example: 1) supervised learning, i.e., where algorithms are

trained with example data, and 2) unsupervised learning, i.e., where algorithms infer a function from unlabeled data. Most machine-learning algorithms are unable to explain their reasoning (e.g., black box).

### Blockchain technologies

The core blockchain technologies<sup>18</sup> are as follows:

- › *Distributed ledger*: a decentralized database where transactions are kept in a shared, replicated, synchronized, distributed bookkeeping record, which is secured by cryptographic sealing. The key attributes are resilience, integrity, transparency, and unchangeability, i.e., mostly “immutable.”
- › *Smart contracts*: are (possibly) computer programs that codify transactions and contracts, which, in turn, “legally” manage the records in a distributed ledger.

Intelligent algorithms and smart contracts will be critical “robo assistants” that run commerce and infrastructure based on distributed ledger technology.

### IoT

The IoT is becoming increasingly crucial because every device that has an on/off switch will have a unique identity, and a connection to the Internet will communicate with and be controlled by an algorithm. Devices range from individual lights in a smart building to domestic appliances to the national infrastructure. When a light fails, an algorithm runs, triggering UBERises, an electrician, to come and

fix the light. The algorithm then pays for the service.

Two important IoT-ecosystem technologies are: 1) building information modeling, which is a digital model of a facility or infrastructure; aside from supporting computer-aided design during construction or refurbishment, the digital model will also be used to manage the facility or infrastructure in real time using IoT resources; and 2) blockchain smart contracts, which will be the algorithms that operate and control the infrastructure.

### Big data (behavioral and predictive) analytics

Big data analytics is the process of examining vast and varied data sets to uncover hidden patterns, trends, customer preferences, and so forth. One of the most exciting areas for intelligent algorithms is behavioral and predictive analytics. Behavioral analytics focuses on providing insight into the actions of people, whereas predictive analytics extracts information from existing data sets to determine patterns and predict future outcomes and trends.

Consider the 2002 film *Minority Report*, an action thriller set in Washington D.C. in 2054, where police utilize algorithms to arrest and convict murderers before they commit their crimes. No longer science fiction, predictive analytics is already being used in the sentencing of offenders, with decisions being challenged in the courts. An example is *Wisconsin v. Loomis*, where Compas, a risk-assessment tool, contributed to the trial judge increasing Loomis’s sentence. This ruling is being appealed because Compas is unable to explain its reasoning, who its creators are, and they are unwilling to divulge its methods due to intellectual property considerations.

In the next section, we look at the evolving algorithm ecosystem and discuss its impact on regulation and the law, that is, algorithms as assistants, competitors, controllers, judge/jury, technology options, and regulations.

## ALGORITHMS AS ASSISTANTS

Traditional (static) algorithms are already prevalent, taken for granted, and perform critical tasks such as flying planes and controlling nuclear systems. The current debate mainly concerns intelligent (dynamic) algorithms, their continued evolution, and potential threat.

Beginning with virtual assistants, known as *chatbots*, these are algorithms designed to simulate a conversation with human users primarily over the Internet, where machine-learning algorithms perform a task, such as providing customer service or answering a question.

Algorithms behind this technology have the capacity for learning, reasoning, and understanding. They range from search engines like Google, to increasingly sophisticated assistants such as Apple Siri, Samsung Bixby with image search, or smart devices such as Amazon Echo/Alexa and Google Home. Regarding liability and the law, if Google returns the wrong answer to a search, we try again. However, if Amazon’s Alexa misinterprets a conversation or hears something on the television and makes an expensive purchase, where does the law stand?

### Rogue algorithms

Rogue algorithms have emerged because of advertisers who abuse Amazon Alexa and Google Home. Recently, Burger King “hijacked” Google Home speakers by creating an ad that triggered devices to read its Wikipedia



entry for the Whopper, edited beforehand to sound like marketing copy. Google quickly blocked the trigger but not before the restaurant chain had gained much free publicity and considerable Google consumer backlash.

Another example is that of Microsoft's Tay, a chatbot algorithm that was designed to learn from user interaction via Twitter. Tay proved a smash hit with racists, trolls, and online troublemakers who persuaded it to blithely use racial slurs, defend white supremacist propaganda, and even call for outright genocide. Even the heavily censored Chinese Internet is not immune: "Rogue Chatbots Deleted in China After Questioning Communist Party," read one recent headline. Two chatbots, BabyQ and XiaoBing, have been pulled from a Chinese messaging app after they questioned the rule of the Communist Party and made unpatriotic comments. The bots were available on a messaging service with 800 million users run by Chinese Internet giant Tencent, before apparently going rogue!

### Regulation and the law

It might be argued that self-regulation works well, based on the chatbot examples mentioned previously. However, it does highlight the significant challenge of testing these evolving machine-learning algorithms.

Although concern has been expressed about the urgent need to police and regulate these rogue algorithms, there exists, through the current U.S. and U.K. criminal and civil laws, a considerable body of law that can be deployed where necessary. Toby Walsh suggests using chatbots-to-humans warnings like the Red Flag Law that governs the early use of motor vehicles ([arxiv.org/pdf/1510.09033.pdf](http://arxiv.org/pdf/1510.09033.pdf)).

## ALGORITHMS AS COMPETITORS

We now examine algorithms that are displacing humans. The application of intelligent algorithms has been driven to a large extent by the highly competitive financial services industry, beginning with algorithmic trading (AT) and the rise of financial robo advisors.

### AT

In electronic financial markets, AT refers to the use of algorithms to automate one or more stages of the trading process, e.g., pretrade analysis (data analysis), trading signal generation (buy and sell recommendations), and trade execution. Each stage of this trading process can be conducted entirely by algorithms or by algorithms plus humans.

**Rogue algorithms.** AT, because of its magnitude and proliferation, has had a significant impact on financial markets. Notably, the 2010 Flash Crash, which wiped out US\$600 billion in market value of U.S. corporate stocks in 20 min. However, the involvement and market impact of AT on flash crashes is still the subject of much debate.

Another interesting example, one that possibly involves a traditional (static) algorithm, is that of market-making firm Knight Capital. On 1 August 2012, Knight Capital deployed untested software in a production environment that contained an obsolete function. The rogue algorithm started pushing erratic trades through on roughly 150 different stocks and lost US\$440 million in 30 min, resulting in the end of the company.

### Professional robo advisors

We now look at how algorithms impact professions. Robo advisors are a class of

advisor software providing professional financial advice or portfolio management with minimal human intervention, based on mathematical rules and AI algorithms. A typical robo collects information from clients about their financial situation, level of acceptable risk, and future goals through an online survey and then uses the data to offer advice and/or automatically invest client assets. There are two broad classes: 1) robo investors, which invest without offering any financial advice and are not formally regulated, and 2) robo advisors, which offer regulated advice to users and then use the responses to guide investment decisions.

**Rogue algorithms.** Warren Buffett, when discussing the aftermath of the 2008 financial crisis, warned, "Wall Street's beautifully designed risk algorithms contributed to the mass murder of [U.S.] \$22 trillion." This comment highlights potential problems, namely that today's robo investors and robo advisor algorithms probably lack the necessary experience to manage assets during sustained periods of market turbulence and falling stocks prices.

### Financial regulations

Regulators are also exploring using algorithms to improve efficiency. Financial regulation is estimated by the *Financial Times* to cost firms billions and involve 10% of the workforce. Regulators face myriad pressures, such as increasing the monitoring of small firms and individuals, cross-border cybercrime (e.g., anti-money-laundering and binary options), political pressure to curb excesses (e.g., Libor), escalating international and EU regulations (e.g., Markets in Financial Instruments Directive II), and governments that relax regulations to increase competitiveness (e.g.,

the Dodd–Frank Wall Street Reform and Consumer Protection Act) and so on.

The monitoring challenges faced by regulators are illustrated by the U.K. Financial Conduct Authority (FCA). Previously, the FCA monitored 25,000 large- and medium-size firms. With virtually the same resources, the FCA now must supervise an additional 30,000 small firms. Hence, regulators are looking to automate compliance and regulations using AI algorithms and blockchain, while also regulating algorithmically. Recently, the U.K. Financial Stability Board published a report<sup>19</sup> about the impact of AI in financial services, pointing out that the lack of “auditability” of intelligent algorithms could become a macrolevel risk.

**Regulation and the law.** Financial algorithms are increasingly subject to compliance, with regulators requiring firms to demonstrate that trading algorithms have been thoroughly tested, demonstrate “best execution,” and are not engaged in market disruption. Likewise, robo advisors are being regulated to benchmark their level of advice to ensure they are not engaged in market manipulation. The U.S. Securities and Exchange Commission requires robo advisors to be registered and compliant in three areas: 1) substance and presentation of disclosures, 2) provision of suitable advice, and 3) enacting effective compliance programs.

With respect to the law, these financial algorithms are not fiduciaries, nor do they currently fit under the traditional standard applied to human registered investment advisors.

## ALGORITHMS IN CONTROL

Although much public debate centers on future intelligent robots, traditional control algorithms are already

omnipresent. An example is an autopilot controlling an aircraft. Suddenly, Asimov’s “Three Laws of Robotics” are a reality, with the proliferation of fully autonomous vehicles and military robots that are designed to kill. Autonomous vehicles have control systems that can analyze sensory data to distinguish between cars on the road, pedestrians, and other potential hazards, which are necessary for safe navigation but also can predict accidents.

The moral dilemma for the software engineer, manufacturer, and regulator are that predictive algorithms may, in extreme situations, need to make life and death decisions. One possible avenue is that a regulator requires navigation software to pass an algorithm “driving test.”

## Rogue algorithms

A recent video on the Internet shows how Tesla’s autopilot algorithm attempts to predict a car accident before it happens. However, not everything is perfect for autopilot algorithms. Nearly every autonomous vehicle company from Tesla and Google to Uber has had some car crashes, including the death of a Tesla driver. Some accidents are algorithm anomalies, some are caused by other drivers’ unpredictable behaviors, and, in the future, some may be caused by malicious hacking.

## Regulation and the law

The law is playing catch up with industrialized countries by adjusting their laws to accommodate autonomous vehicles. For example, the U.K. Vehicle Technology and Aviation Bill imposes liability on the owner of an uninsured automated vehicle when driving itself and makes provisions for cases where the owner has made “unauthorized alterations” to the vehicle or failed to update its software.

Likewise, no one expects the law to condone autonomous vehicles driving drunks home! However, challenging legal questions are already being posed as to what happens where there are collisions between two driverless cars and both appear to have acted appropriately. Further ethical issues arise when, e.g., a driverless car swerves to avoid a pedestrian and causes a fatal accident.

## ALGORITHMS AS JUDGE AND JURY

Perhaps the most contentious area is algorithms making decisions regarding humans with little or no right of appeal. This includes: 1) consumer decisions, where applicants are judged by algorithms that are unable to explain their reasoning, ranging from CV-sifting software to people applying for loans and mortgages; 2) staff decisions, where algorithms select staff for jobs, decide remuneration, and whether they should be dismissed; and 3) defendant decisions, where the justice system is using algorithms to recommend sentencing of criminals. As previously discussed, one example is *Wisconsin v. Loomis*, where a black-box risk-assessment tool contributed to the trial judge increasing Loomis’s sentence.

## Algorithmic star chamber

In the workplace, algorithms are rapidly becoming a judge and jury “star chamber.” Uber has been criticized in the media for only communicating with its drivers via algorithms that unilaterally decide on the level of revenue share, driver’s rating, and whether to terminate employment without the right of appeal. Online retailers live in fear of a drop in their Google search-engine ranking if they are judged by an algorithm to have done something fraudulently.

### Rogue algorithms

Engineers creating algorithms face increasing ethical and legal challenges that can have severe consequences affecting individuals, groups, and whole societies. As an example, consider the following: you have been asked to code the algorithm for a self-driving car that can predict possible accidents. When a fatal accident appears unavoidable, does your algorithm 1) sacrifice the car, 2) sacrifice the pedestrian, 3) sacrifice passengers in other vehicles, 4) risk harming the occupants, or 5) risk an even greater accident?

### BLOCKCHAIN SMART CONTRACTS

We now consider the emerging technology of smart contracts, one of the most contentious algorithm technologies for lawyers, and frequently disparaged as “not smart, not contracts.”

However, to quote Sean Murphy<sup>20</sup> of Norton Rose Fulbright, “Smart contracts, in combination with distributed ledger technologies, have the potential to automate an extensive array of transactions and services within the service sector. Legal compliance can be built into the program logic, providing a way of transacting that maximizes operational efficiencies with the potential to reduce legal and regulatory cost and risk.”

### Regulation and the law

With regard to smart contract law, proponents fall into three legal camps: 1) code-is-contract, i.e., those who espouse encoding the entirety of a natural language contract; 2) hybrid-contract, i.e., those using a hybrid smart contract model under which natural language contract terms are connected to computer code via parameters (e.g., a smart contract template) that feed

into computer systems for execution; and 3) code-is-business-logic, i.e., those who see smart contracts as consisting of digitizing business logic performance (e.g., payment), which may or may not be associated with a natural language contract.

### TECHNOLOGY OPTIONS

Before discussing regulatory structures and possible changes to the law, it is appropriate to discuss technology options.

#### Algorithm testing

Depending on the nature of the system, techniques divide into the following:

- › *Traditional testing*, which can involve static code reviews or dynamic analysis with test sets, along with “white-box” internal workings and “black-box” functionality
- › *Algorithm formal verification*, which proves or disproves the correctness using a formal proof on an abstract mathematical model of the system, which corresponds accurately to the nature of the system (usually known before construction).
- › *Algorithm cross-validation*, which aims to run the same algorithm in an independent data set or scenario to evaluate potential risks (e.g., overfitting, sensitivities to noise, and so on) and measure its expected generalization accuracy.

#### Algorithm certification

Algorithm certification involves auditing whether the algorithm used during the life cycle 1) conforms to the protocol requirements (e.g., for correctness, completeness, consistency, and

accuracy); 2) satisfies the standards, practices, and conventions; and 3) solves the right problem (e.g., correctly model physical laws), and satisfies the intended use and user needs in the operational environment.

### Algorithm circuit breakers

For financial algorithms, circuit breakers are used to detect failures and encapsulate the logic by preventing a failure from regularly recurring during maintenance, temporary external system failures, or unexpected system difficulties. Circuit breakers are used by exchanges to curb panic selling and excessive volatility (i.e., large price swings in either direction) in individual securities. For machine-learning algorithms circuit breaker technology, monitoring functionality may be the only option.

Arguably, algorithm testing and algorithm certification are unlikely to fully work for machine-learning algorithms. As a result, all critical intelligent algorithms may require circuit breakers.

**L**egal redress for algorithm failure seems straightforward: if something goes wrong with an algorithm, just sue the humans who deployed the algorithm. However, it may not be that simple. For example, if an autonomous vehicle causes death, does the lawsuit pursue the dealership, the manufacturer, the third-party who developed the algorithm, the driver, or the other person’s illegal behavior? This stimulates the debate of whether or not algorithms should be given a legal personality.

As we know, a *legal person* refers to a nonhuman entity that has legal standing in the eyes of the law. A graphic example of a company having legal

personality is the offense of corporate manslaughter, which is the criminal offense of an act of homicide committed by a company or organization. Another important principle of law is that of agency, in which a relationship is created whereby a principal gives legal authority to an agent to act on the principal's behalf when dealing with a third party. An agency relationship is a fiduciary relationship. It is a complex area of law with concepts such as apparent authority, where a reasonable third party would understand that the agent had authority to act.

As the combination of software and hardware continues to produce intelligent algorithms that learn from their environment and may become unpredictable, it is conceivable that, with the growth of multialgorithm systems, decisions will be made by algorithms that have far-reaching consequences for humans. It is this potential of unpredictability that supports the argument that algorithms should have a separate legal identity so that due process can occur in cases where unfairness is present. The alternative to this approach would be to adopt a regime of strict liability for those who design or place dangerous algorithms on the market, so as to deter behaviors that appear or are proved to have been reckless. Is this a case of bolting the barn door after the horse has escaped?

We present three discussion points:

- *Algorithm circuit breakers:* Critical intelligent algorithms may require mandatory circuit breakers for safe operation because algorithms with machine learning evolve dynamically and may prove unfeasible to rigorously test and verify.
- *National algorithm safety board:* A special national board will

be required to provide expert knowledge and advice.


- *Legal status of algorithms:* Currently, algorithms are not considered to be artificial persons, i.e., “they are unable to own things so they are not worth suing.” However, in cases where dynamic algorithms and robots develop beyond the intentions of the designers, where the owner/designer of an algorithm cannot be identified (perhaps through insolvency), or where a so-called decentralized autonomous organization builds a store of wealth, a body of opinion is forming in law to support the view that courts should have the ultimate authority to issue sanctions, which might include the power to fine or use a “kill switch” where necessary.

In summation, Ben Shneiderman has called for a national algorithm safety board.<sup>2</sup> Such a board would have the expertise to 1) provide specialist advice on algorithms to sectors such as finance and 2) recommend changes to the law as algorithms and their ecosystem evolve. A proposed codes of ethics for designers of algorithms do not yet suggest how these principles can be enforced, giving rise to a need for a debate concerning potential sanctions for its breach.

Regarding giving algorithms a legal personality (i.e., artificial persons), a company having legal personality can, for example, be charged with corporate manslaughter, which is a criminal offence in law. Another controversial issue in law is called *Agency*; wherein algorithms are authorized to enter into contracts with humans or other algorithms and subsequently a dispute

arises about the scope of the algorithms' authority. This article was written to stimulate discussion in the computer science and legal professions concerning algorithms, regulations, and the law, a subject of growing debate.

## ACKNOWLEDGMENTS

We thank the reviewers for their comments and ideas that have helped us reshape and improve our article. 

## REFERENCES

1. O. Etzioni, “How to regulate artificial intelligence,” *NY Times*, Sept. 1, 2017. [Online]. Available: <http://www.nytimes.com/2017/09/01/opinion/artificial-intelligence-regulations-rules.htm>
2. B. Shneiderman. (2017). “Turing lecture on algorithm accountability,” Turing. Accessed on: Jan. 2019. [Online]. Available: [www.turing.ac.uk/events/turing-lecture-algorithmic-accountability/](http://www.turing.ac.uk/events/turing-lecture-algorithmic-accountability/)
3. S. Spiekermann, “Artificial intelligence: Considering the ethics,” *Parliament Mag.*, Nov. 7, 2016. [Online]. Available: <https://www.theparliamentmagazine.eu/articles/magazines/ieee-considering-ethics>
4. IEEE. (2018). IEEE P7000—Engineering methodologies for ethical life-cycle concerns working group. IEEE. Piscataway, NJ. [Online]. Available: <http://sites.ieee.org/sagroups-7000/>
5. C. O’Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Largo, MD: Crown Books, 2017.
6. F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money And Information*. Cambridge, MA: Harvard Univ. Press, 2015.



## ABOUT THE AUTHORS

**PHILIP TRELEAVEN** is a professor of computing at University College London and director at the U.K. Centre for Financial Computing & Analytics ([www.financialcomputing.org](http://www.financialcomputing.org)). His research interests include data science, algorithms, and blockchain technologies. Treleaven received a Ph.D. from The University of Manchester. He is a Member of the IEEE and the IEEE Computer Society. Contact him at [p.treleaven@ucl.ac.uk](mailto:p.treleaven@ucl.ac.uk).

**JEREMY BARNETT** is a regulatory barrister and sits as a Recorder of the Crown and County Court, St. Paul's Chambers ([www.stpaulschambers.com/jeremy-barnett-crime](http://www.stpaulschambers.com/jeremy-barnett-crime)) and Gough Square Chambers. Barnett received his L.L.B. from the University of Liverpool. With a background in advanced computing, he is currently involved in research and development of blockchain and smart contracts. Contact him at [Jeremy.Barnett@Resilience-Partners.co.uk](mailto:Jeremy.Barnett@Resilience-Partners.co.uk).

**ADRIANO KOSHIYAMA** is a Ph.D. student at University College London in the Department of Computer Science. Koshiyama received his M.Sc. in electrical engineering from PUC-Rio. His research interests include computational finance and AI. He is a Student Member of the IEEE and the IEEE Computer Society. Contact him at [adriano.koshiyama.15@ucl.ac.uk](mailto:adriano.koshiyama.15@ucl.ac.uk).

7. N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*. London, U.K.: Oxford Univ. Press, 2014.
8. B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, "The ethics of algorithms: Mapping the debate," *Big Data Soc.*, vol. 3, no. 2, 2016.
9. M. J. Kusner, J. Loftus, C. Russell, and R. Silva, "Counterfactual fairness," *Advances Neural Inform. Process. Syst.*, vol. 2016, pp. 4069–4079, 2017.
10. EUR-Lex. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). European Union. Brussels, Belgium. [Online]. Available: <http://eur-lex.europa.eu/eli/reg/2016/679/oj>
11. S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the general data protection regulation," *Int. Data Privacy Law*, vol. 7, no. 2, pp. 76–99, 2017.
12. A. Tutt, "An FDA for algorithms," *Administ. Law Rev.*, vol. 69, no. 83, pp. 83–125, 2017.
13. J. Taylor, E. Yudkowsky, P. LaVictoire, and A. Critch, *Alignment for Advanced Machine Learning Systems*. Berkeley, California: Machine Intelligence Research Institute, 2016.
14. D. Amodei, C. Olah, J. Steinhardt, P. Christiano, J. Schulman, and D. Mané, "Concrete problems in AI safety," 2016. [Online]. Available: [arXiv:1606.06565](https://arxiv.org/abs/1606.06565)
15. J. Leike et al., "AI safety grid-worlds," 2017. [Online]. Available: [arXiv:1711.09883](https://arxiv.org/abs/1711.09883)
16. S. Hawking, M. Tegmark, S. Russel, and F. Wilczek, "Transcending complacency on superintelligent machines," *Huffington Post*, June 19, 2014. [Online]. Available: [http://www.huffingtonpost.com/stephen-hawking/artificial-intelligence\\_b\\_5174265.html](http://www.huffingtonpost.com/stephen-hawking/artificial-intelligence_b_5174265.html)
17. S. Russell, D. Dewey, and M. Tegmark, "Research priorities for robust and beneficial artificial intelligence," *AI Mag.*, vol. 36, no. 4, pp. 105–114, 2015.
18. P. Treleaven, R. G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.
19. Financial Stability Board. (2017). Artificial intelligence and machine learning in financial services. FSB. Basel, Switzerland. [Online]. Available: <http://www.fsb.org/2017/11/artificial-intelligence-and-machine-learning-in-financial-service/>
20. S. Murphy and C. Cooper, "Can smart contracts be legally binding contracts?" Norton Rose Fulbright, London, U.K., White Paper, 2016.
21. IEEE. (2016). Ethically aligned design: A vision for prioritizing human well-being with artificial intelligence and autonomous systems. IEEE. Piscataway, NJ. [Online]. Available: [http://standards.ieee.org/develop/indconn/ec/ead\\_v1.pdf](http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf)



IEEE COMPUTER SOCIETY

**DIGITAL LIBRARY**

Access all your IEEE Computer Society subscriptions at

**computer.org**  
**/mysubscriptions**