Technology, institutions and regulation
towards a normative theory

Smith, Marcus; Miller, Seumas

DOI
10.1007/s00146-023-01803-0

Publication date
2025

Document Version
Final published version

Published in
AI and Society

Citation (APA)
Smith, M., & Miller, S. (2025). Technology, institutions and regulation: towards a normative theory. *AI and Society*, *40*(2), 1007-1017. https://doi.org/10.1007/s00146-023-01803-0

AI & SOCIETY (2025) 40:1007–1017
https://doi.org/10.1007/s00146-023-01803-0

OPEN FORUM

Technology, institutions and regulation: towards a normative theory

Marcus Smith[1] · Seumas Miller[1,2]

Received: 10 May 2023 / Accepted: 16 October 2023 / Published online: 28 November 2023

Abstract

Technology regulation is one of the most important public policy issues facing society and governments at the present time, and further clarity could improve decision making in this complex and challenging area. Since the rise of the internet in the late 1990s, a number of approaches to technology regulation have been proposed, prompted by the associated changes in society, business and law that this development brought with it. However, over the past decade, the impact of technology has been profound and the associated issues for government have extremely challenging, ranging across cyber security, artificial intelligence, and many other areas. To that end, this article introduces a Theory of Institutional Technology Actors and Norms (TITAN), a normatively informed and institutionally-based account of technology regulation. It focuses on the moral and legal (including regulatory) rights and responsibilities of the relevant actors and seeks to inform the development of regulation that is both fit for purpose, rights compliant and fair for all concerned. The account incorporates the perspectives of four key categories of groups in society: producers of technology, users of technology, government regulators, and normative policy shapers.

Keywords Technology regulation · Ethics · Law reform

1 Introduction

Technology regulation is one of the most important public policy issues facing society and governments at the present time, and further clarity could improve decision making in this complex and challenging area (Buitten 2019; Ulnicane et al. 2020). Because the rise of the internet in the late 1990s, a number of approaches to technology regulation have been proposed, prompted by the associated changes in society, business and law that this development brought with it (e.g. Lessig 1999; Murray 2007). However, over the past decade, the impact of technology has been profound and the associated issues for government have been extremely challenging, ranging across artificial intelligence, cybersecurity and more specific issues such as autonomous cars (Wirtz et al. 2020). These examples will be explored later in this article. The existing approaches have focused on the internet and lack the flexibility to be applied across the wide range of technologies in use today. There is; therefore, a need for novel theoretical approaches that can be used to inform technology regulation (Smith and Urbas 2021).

To that end, this article introduces a Theory of Institutional Technology Actors and Norms (TITAN). The theory sets out a normatively informed and institutionally-based account of technology regulation. It focuses on the moral and legal (including regulatory) rights and responsibilities of the relevant actors and seeks to inform the development of regulation that is both fit for purpose, rights compliant and fair for all concerned. The account incorporates the perspectives of four key categories of groups in society relevant to this domain: (1) Producers of technology, i.e., scientists, technology companies etc.; (2) Users of technology, i.e., ordinary citizens, industries; (3) Government regulators of technology, i.e., legislators, regulatory bodies, public policymakers; (4) Normative policy shapers, i.e. ethicists, professional standards bodies and legal professionals–groups within each category occupy a role that needs to be considered in the decision-making process in relation to technology regulation. Here we note in relation to the fourth category, normative policy shapers, that good public policy relies not only on empirical input and political feasibility but also on

✉ Marcus Smith
marcussmith@csu.edu.au

✉ Seumas Miller
semiller@csu.edu.au

[1] Charles Sturt University, Canberra, Australia

[2] Delft University of Technology, Delft, Netherlands

normative input and, crucially, ethical and legal principles; hence, the need for ethicists and lawyers to provide input that shapes technology regulation.

TITAN incorporates two theoretical notions. First, there is normative institutional theory. Technology is embedded in fundamental institutions that typically have prior roles to deliver collective goods for the benefit of society; these goods include security (law enforcement agencies), health (hospitals), electricity (power generators and infrastructure), and so on. Normative institutional theory identifies and elaborates these collective goods and, thereby, gives direction to institutions. For instance, law enforcement agencies ought to have as a principal institutional purpose to secure the legally enshrined moral rights of citizens. However, the interaction between fundamental institutions and the citizens, groups and organisations that they serve (or otherwise engage with) is mediated and shaped by technology. Moreover, technology is embedded in these institutions and; therefore, embedded in the wider society; indeed, technology in part constitutes institutions and the wider society (Hirvonen 2023). Consider in this connection the internet; it now mediates and shapes a great deal of private and public communication and is in part constitutive of, for instance, social media companies, educational institutions, law enforcement, government agencies, businesses etc. Hence, the regulation has the role of ensuring that technology is appropriately institutionally embedded, and that technology mediates and shapes the interaction between institutions and those that they serve (or otherwise engage with) in an appropriate manner. What is or is not appropriate is in large part a matter of whether the technology in question facilitates the collective good(s) produced or maintained by the relevant fundament institutions and does so in an effective, lawful and ethically sustainable manner. Note that what is lawful ought itself to reflect basic ethical principles, such as individual autonomy and privacy.

Our second theoretical notion is collective responsibility. Researching, developing, regulating and using technology involves multiple actors all of whom have a share in the collective responsibility to ensure, in part by means of regulation, that technology is produced and used in an effective, lawful and ethically responsible manner. Of course, there are two conceptually separable but, nevertheless, interconnected issues here. Firstly, there is the collective responsibility to ensure that technology is produced and used in an effective, lawful and ethically responsible manner. Secondly, there is the collective responsibility to ensure that an important means to this end, namely, regulation itself is effective, lawful (e.g., in terms of human rights legislation) and ethically sustainable. It might be thought that it is only the members of governments, especially legislators and regulators, that have a collective responsibility in relation to devising and implementing regulation. Naturally, they have a larger responsibility in this regard than others. However, all groups within our four groups have responsibilities with respect to regulation, even if only in so far as they need to comply with it in order to ensure it is effective, as in the case of ordinary citizens. That said, while regulation is ultimately an important, indeed necessary, means to the overarching end of technology, it is not the only necessary means. Moreover, obviously, members of groups in the other three categories have different responsibilities in respect of other necessary means in relation to the realisation of the end of, for instance, seeing to it that technology facilitates collective goods. Consider, for instance, scientists and technology companies producing new biotechnology to facilitate public health. Naturally, to reiterate, in doing so they need to comply with regulation. However, we also suggest that they ought to provide input to government in relation to regulatory policy relevant to biotechnology.

TITAN's recourse to the above-mentioned four categories of groups enables us to describe the main contributors or, at least, potential contributors, to contemporary issues in technology regulation. Recourse to the two above-mentioned theoretical notions enables us provide normative direction to technology regulation. Our overall account is useful at two levels: first, to understand complex macro level policy problems requiring the consideration and integration of new technologies and the assessment of scientific knowledge, to formulate appropriate policy settings and develop regulation for specific types of new technology; second, to give normative direction to such policy settings and regulation and do so in light of our two theoretical notions (normative institutional theory and collective responsibility).

In proposing this new theoretical account, the article is divided into three parts. The first provides context, discussing the growing importance of technology regulation, and outlining a number of theoretical approaches that have been proposed to date. The second describes the four categories of groups of actors we argue must be considered in the analysing problems of technology regulation, and develops the theory from the perspectives of group interdependence and collective goods. The third section provides two contemporary examples of contemporary problems in technology regulation, cybersecurity and artificial intelligence, and discusses them in light of the TITAN approach we have outlined, highlighting the role of normative institutions and collective responsibility, and its importance to appropriate regulation.

2 Technology regulation

The regulation of technology is an increasingly important ethical, legal and social issue. It is a complex undertaking and requires an appreciation of underlying scientific knowledge (which continues to evolve), ethical principles and law reform strategies: issues are fast moving and often extend across multiple international jurisdictions (Buitten 2019). Technological developments in countries with significant innovation and commercial development, such as the United States and China, rapidly have international ramifications, due to the connectedness facilitated by the internet and modern communications technology. New technologies regularly create regulatory gaps and inequalities; but are associated with improved efficiency, reduced costs, and greater access to knowledge and business opportunities (Hirvonen 2023). The recent examples are the emergence of cryptocurrencies such as Bitcoin, which challenged the existing laws and financial regulations, requiring new guidelines as to whether they constitute forms of currency and are subject to taxation; advancements in artificial intelligence, which have required that established legal principles of responsibility and liability be reconsidered; and managing public safety and individual rights in responding to the COVID-19 pandemic with the rapid development of mRNA vaccines and contact tracing applications.

With such a wide range of different technologies requiring regulation, each being used in various contexts, with multifaceted risks and benefits needing to be balanced to prevent harms. Adequate regulation, in the form of legislation, judicial oversight, policies, standards and procedures, spans various areas of the legal system, fields of business, government agencies, and state, national and international jurisdictions, equating to a major challenge for regulators to establish a coherent, consistent, effective and ethically sustainable control of new technologies (Guihot et al. 2017). The complexity in understanding the technology itself is added to by the pace at which new technologies are developed, and the breadth of their impact. Brownsword et al. (2017) propose that technology regulation must address three aspects: the challenge that new forms of technology pose to 'established legal frameworks, doctrines, and institutions', the 'adequacy of existing regulatory regimes', and the 'ideas and justifications offered in support of regulatory intervention'. An important component of the latter 'ideas and justifications' aspect is the ethical or moral (we use these terms interchangeably) one. Regulatory intervention must satisfy, for instance, the demands of various individual moral rights, such as privacy and autonomy rights.

Moreover, ultimately, technology interventions must be in the service of social, economic and other collective benefits (collective goods, in our parlance). Many collective benefits may also be collective goods; but some might not since they might not be goods objectively speaking. For instance, cybertechnology should facilitate public communication but do so in a manner does not unacceptably infringe the right to privacy or undermine social norms of truth-telling (Smith and Urbas 2022). Cybertechnology is mediated and shaped by, and embedded in, various institutions, including but not restricted to, multinational corporations, such as Meta, Alphabet, Twitter and TikTok, that provide platforms for public communication. Thus, seeing to it that cybertechnology facilitates public communication depends in part in ensuring by means of regulation, and perhaps institutional redesign, that cybertechnology is mediated and shaped by, and embedded in, those institutions in a manner that facilitates public communication and does not corrupt or otherwise undermine it. This requires in turn that regulation ensures that cybertechnology is not mediated or shaped by, or embedded in, these institutions in a manner that undermines compliance with the moral and epistemic norms, such as truth-telling and trust, that not only counter the corruption of public communication by disinformation inter alia but, ultimately, enable public communication. These norms enable public communication in that if there was to be wholesale abandonment of, for instance, the norms of truth-telling and trust then effective public communication would cease to be possible since the channels of public communication could not be relied upon to provide the truths being sought (Smith and Urbas 2022).

Over the past decade, a growing number of policy issues engage with technology and regulation. They are associated with a weighing of priorities at the heart of many issues in technology regulation, a trade-off between individual rights and collective goods, the need to regulate the harmful aspects of new technology and the associated challenges inherent in doing so, while facilitating the development and adoption of beneficial technological advancements. The vast advances in information and communications technology have been associated with compromised privacy and autonomy, principally due to the development of the internet, smartphones and social media, highlighted by events such as the Snowden disclosures, and the Cambridge Analytica affair. Fields in society where the complex implications of new technology can be observed include genomics, cybercrime, biometrics and artificial intelligence.

The rise of the internet in the late 1990s was a significant technological development that presented one of the most significant regulatory challenges in history, through its capacity to transmit information around the world instantaneously—a development that continues to have a profound effect. It was quickly evident that traditional, state-based sovereignty and legal jurisdiction would be challenged in cyberspace:

> Clear boundaries make law possible, encouraging rapid differentiation between rule sets and defining the subjects of legal discussion. New abilities to travel or exchange information rapidly across old borders may change the legal frame of reference and require fundamental changes in legal institutions. Fundamental activities of lawmaking – accommodating conflicting

> claims, defining property rights, establishing rules to guide conduct, enforcing those rules, and resolving disputes – remain very much alive within the newly defined, intangible territory of cyberspace. At the same time, the newly emerging law challenges the core idea of a current law-making authority – the territorial nation state, with substantial, but legally restrained powers (Johnson and Post 1996).

This led to new ideas in regulation. In seeking to adapt regulatory processes for cyberspace, involving states, citizens, the private sector and the technology itself, Reidenberg developed the concept of *Lex Informatica*, referring to 'laws' imposed by technological capabilities and system designs, focusing on the regulation of the internet using its inherent architecture, rather than by proscribing particular activities an individual can undertake:

> …law and government regulation are not the only source of rule-making. Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations…the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica' that policymakers must understand, consciously recognize, and encourage (Reidenberg 1998).

A similar approach was advanced by Lessig in his influential work *Code*. He argued that cyberspace can be regulated through four 'modalities of regulation': the law, social norms, market forces, and architecture (Lessig 1999). We note that markets are one form of human institution; there are other non-market-based institutions, such as schools, universities, religious institutions and institutions of democratic governance. These also ought, presumably, to be regarded as part of Lessig's modalities of regulation. At any rate regulators apply combinations of these modalities in a direct or indirect way to control the activities of individuals, in both real world and digital contexts. The law controls individual activities through the threat of legal sanctions such as fines or imprisonment, social norms through the threat of social sanctions such as stigma, the market through pricing, schools and universities through processes of learning (and so on and so forth for other institutions), and architecture (code) through physical constraints such as a firewall or a requirement that internet service providers block illegal websites.

Lessig describes the individual as a dot controlled by these modalities–whilst it may be difficult for traditional law to regulate the internet, when law is combined in a regulatory framework, it becomes feasible. The advantage of using architecture (or code) for regulation is that it has a high level of compliance, as the vast majority of the population lacks the technical skills to circumvent it. The approach physically prevents non-compliance and is a low-cost option for the government to administer because the costs are often borne by the private sector in building systems that comply with regulatory requirements. In contrast with enacting laws, it can often be done without even informing the public that it has been implemented. This aspect raises questions of transparency in liberal democracies: '…it muddies the responsibility for that constraint and so undermines political accountability' (Lessig 1999; 96).

Lessig's model has been developed into a wider theory, with the dot forming a node in a network described as an 'active dot matrix' (Murray 2007). The dot is an active part of a regulatory process that is a 'dialogue, not an externally imposed set of constraints' (Murray 2019). This form of symbiotic regulation, where the regulator takes the views of the community into account and formulates an approach they are likely to accept, is mutually beneficial for the regulator and the community. Murray terms this approach 'network communitarianism', contrasting it with Lessig's 'cyberpaternalism':

> Cyberpaternalism proposes coercion, whereas network communitarianism suggests incentivisation and persuasion. In cyber paternalism the dot (or dots) acts in a certain way because of 'constraint', whilst in network communitarianism it does so because of 'encouragement' (Reed and Murray 2018).

Appropriately understood, or perhaps revised, cyberpaternalism and network communitarianism are not necessarily inconsistent with one another, although they have difference emphases. A strength of network communitarianism is that it implicitly, at least, acknowledges the limitations of coercion. A strength of cyberpaternalism is that it acknowledges the necessity of coercion. Arguably, both approaches need to acknowledge the limitations of 'social engineering' in whatever form it takes. For instance, ultimately regulators cannot regulate fundamental social norms, such as trust or respect for privacy and autonomy, into existence, although they can buttress them.

Twenty years after the internet began to be widely used, it is now an established part of business and daily communication, providing the foundation for an ever-expanding array of new technologies. From smartphones and associated apps, to digital health records, bitcoin, blockchain and online businesses, the internet has provided a platform for modern technology development. Technology regulation must continue to evolve to respond to modern technology, building on the work of Reidenberg, Lessig and Murray. Regulatory theory should recognise not only the way the different groups and modalities operate collectively to influence the behaviour of individuals and other stakeholders in society, but the way these actors interact and shape each other. The notion of collective responsibility has been used by ethicists to understand the moral and regulatory implications of a range of technologies, such as bulk databases (Miller and Bossomaier 2022), financial infrastructure (e.g., financial benchmarks), blockchain, dual use technology (including cyber, nuclear, chemical and biotechnology) (Miller 2018) and autonomous weapons (Miller 2016), and also to assist in elucidating these issues when applied to of the issue of technology regulation more broadly. Institutional theory has been used to help understand the relationships between technologies and their producers and users, given technology production and use is necessarily mediated and shaped by institutions and, indeed, embedded in institutions.

In the information technology field, there has been a wide-ranging discussion of norms by a several influential theorists over the past fifty years. These includes Stamper's computerised representation of the law, LEGOL (LEGally Oriented Language), and MEASUR (Methods for Eliciting, Analysing and Specifying Users' Requirements) methodologies (Stamper 1977; Stamper et al. 1988). Earlier in the 1970's, Habermas wrote about the role of norms in the public sphere, and specifically in relation to the role of science and technology in society (Habermas 1970). The term 'norm' has been used in multiple ways. In this article, our concern is fundamentally with the ethical norms and legal norms in relation to new technology that prescribe or proscribe certain actions. As with norms, definitions and accounts of regulation are vast. In order not to detract from the key points of the theoretical account set out here, we must be selective and have, therefore, focused on the most significant, recent and directly relevant accounts that have influenced our approach. But we note that normative institutional theory can give direction to regulators of technology, as we argue below.

3 Technology actors

3.1 Group interdependence

As noted in the introduction, our TITAN account of technology regulation proposes four key categories of groups of actors impacted by new technology, that need to be considered in understanding how a particular type of technology should be regulated, and limiting the circumstances under which it can be used: (1) The Producers of technology, i.e. (i) the scientists (including engineers and information technology professionals) that develop the technology through their knowledge, training, expertise and innovation, and provision of advice in relation to its capabilities and how it can be used; (ii) the technology companies that invest in and develop new technology products or services, and take these to market, serving consumers and generating profits; (2) The Users of technology, i.e., (i) ordinary citizens and (iii) businesses and public sector agencies, who are the end users/consumers of technology, or upon which technology is applied by companies, governments or other citizen users; and (3) Government regulators of technology: legislators, regulators and public policy makers, that regulate technology through legislation and regulation; (4) Normative policy shapers: (i) the ethicists who can analyse and propose ethically defensible options as well as ethical constraints, (ii) professional standards bodies, and (iii) the legal professionals (including lawyers and judicial officers) that provide advice to government, companies and individuals, and in the case of judges, interpret relevant legislation and case law, and resolve disputes. The problem of technology regulation is to consider how these four categories of groups act, and are acted upon, to regulate technology and, crucially for our purposes here, define and balance the rights and responsibilities of these groups in respect of technology regulation.

An example of interdependence between members of a group and across members of groups, can be illustrated by taking an electric vehicle as an example. Let us suppose that electric cars are an efficient, effective and ethically sustainable form of transport that can meet aggregate demand on a large scale as well as radically reduce pollution, thereby contributing to the saving the planet from disastrous climate change. Electric cars promise to deliver a number of important collective goods (Meckling and Nahm 2018). An electric vehicle manufacturer is reliant on research, development, implementation and advice from scientists and engineers, other companies to provide components of their cars, and on governments to register their cars for use, and build roads. Without computer hardware, GPS satellites, research that has reduced the size of batteries and increased their storage capacity, mining companies to provide raw materials such as iron, lithium, nickel and cobalt, and basic infrastructure provided by governments, electric vehicle companies could not develop and offer a valuable product to their customers. If an electric vehicle has not been tested and registered by a government who allows it to be driven on its roads, it has little value to a consumer, or consequently to a company if it cannot profit from its sale.

Individuals and society gain collective goods such as cheaper, cleaner, more efficient private transport on a large scale, but they must also consider how their location and other data collected by sophisticated electric vehicles may impact on their privacy, and how autonomous systems may impact their safety. The company itself must comply with privacy laws and not unreasonably exploit personal data; computer scientists employed by the company are responsible for providing advice and implementing systems to maintain data security and user safety; and state, federal and international governments around the world must collaborate in enacting legislation that regulates a large multinational company that may be headquartered in the United States but operates in hundreds of different jurisdictions with differing legal systems.

This is the case for many technologies. Without the computers or smartphones generated by technology companies, Internet companies such as Google cannot serve to provide access to information or generate advertising revenue. A smartphone without a connection to a telecommunications network cannot send text messages or receive phone calls and cannot access the Internet or social networking applications. It can record video or a picture but not share or communicate it. Google requires computer scientists to develop and maintain the site; private citizens to upload content and connect to other citizens, which is all founded on governments upholding a sufficiently orderly society to enable the economy to function effectively.

3.2 Collective goods

In designing appropriate technology regulation, the benefits and risks associated with each of these four categories of groups (producers, users, regulators and policy shapers) must be taken into consideration, and the competing priorities managed. There are the collective goods that technology companies provide: the aggregate of devices and systems they sell increase business efficiency, make personal tasks easier and more convenient for large numbers of users, and add to the enjoyment of life for most members of many, if not most, nation-states through recreational activities and greater opportunities to communicate with others around the world. Rapid increases in the accessibility of information, facilitated by the internet, has had a profound impact on business productivity and living standards over recent decades. However, there are also risks and potential for harm through the loss of privacy rights, and opportunities for bad actors to access personal and financial data and commit identity theft or undertake a ransomware attack etc. Automation and more efficient business practices has reduced employment opportunities in traditional fields and shifted administrative roles to developing countries where labour costs are lower. Global operation also increases the risk of tax avoidance and lower revenues for government, one consequence of the vast size of multinational technology companies, and their bargaining power relative to individuals, smaller business, and indeed governments and regulatory agencies.

An initial question to be asked in respect of any new technology is what is its purpose and, more specifically, what is its benefit to society. In terms of our normative institutional theory, the benefit to society is to be understood as a collective good, such as efficient, effective and ethically sustainable public communication (Miller 2010, 2015). Many collective goods in our sense are also public goods in the economists' sense of that term, i.e., they are non-rival and non-excludable.[1] However, collective goods in our sense are goods that are jointly produced or maintained; clearly goods that are produced by technology are goods in this sense, given (as we have seen) multiple actors are involved in the design, development and so on of technology.[2] Moreover, collective goods are goods for large numbers of people and, in relation to the collective goods in question here, they rely on technology; the joint productive action, and the aggregate consumption, of these collective goods is heavily reliant on technology, albeit in a variety of ways. Thus, the totality of users (drivers) of autonomous electric cars are consumers of a collective good; the aggregate of autonomous electric cars jointly produced by scientists and car manufacturers. Moreover, this productive activity and the uses of the technology (autonomous electric cars) are constrained in various ways by ethically informed regulation, e.g. with respect to safety, that is devised by legislators, regulatorsand (ideally) normative policy shapers (lawyers, ethicists).

Here it is important to note that there are generic collective goods, such as better communication (e.g., internet, Wi-Fi and messaging services), and more specific collective goods, such as more secure phone communications (e.g. end-to-end encryption). Moreover, the specific collective good varies according to the specific technology, but generally involves (in relation to previous technology) a saving in terms of money or time, or a new capability to obtain information, communicate, travel, obtain or provide services etc. Moreover, while there are a variety of collective goods, in the context of our discussion of technology they share a couple of things in common by virtue of being collective goods. Firstly, the notion of a good in play here is that of an objective good as opposed to, for instance, a mere desire. Thus, cyber weapons may be used for the *desired* destruction of critical infrastructure but this would not render this outcome a good, objectively speaking. Secondly, the collective goods in question are not only jointly produced by multiple actors, albeit by recourse to technological means, those who produce them, and perhaps also those who use them, e.g., if the good in question is one to which persons have a prior moral right such as clean water or (in modern societies) internet access, have a joint right to the benefits thus produced or, at the very least, to remuneration for producing

[1] A non-rival good is one that can be consumed or used by multiple persons; a non-excludable good is one that it is costly or impossible to exclude others from its consumption or other use.

[2] As mentioned above, many goods that might be thought to be collective goods, in some sense, are not produced, e.g. the atmosphere. Moreover, a good can be a collective god in our sense without being non-rival or non-excludable, i.e. without being public goods in the economist's sense since collective goods in our sense can be aggregate of goods such as, for instance, the supply of housing in a city.

them. Accordingly, the design and production of this enabling technology is a joint i.e., cooperative, enterprise, that produces or maintains a collective good to which there is a joint right. Hence, the goods technology produces or maintains are collective goods, at least in this sense.

A collective good in and of itself provides an incentive to design and produce the technological means to realise that good. Nevertheless, as mentioned above, those who jointly produce or maintain a collective good have a joint right to the good, e.g., a property right or, even if not, at least a joint right to some reward for their efforts. Correspondingly,, other things being equal, the users or consumers of that good, typically a product or service, whether they be private citizens or governments or other institutional actors, must be willing to pay for it (or exchange something of value for it, such as their metadata) in order for it to have monetary value. In turn, a company must pay scientists for their expertise to develop the technology and advice in relation to how it is used. Finally, the legislature must be convinced that a technology does in fact produce or maintain a collective good for the community that is not outweighed by a potential attendant harm associated with it or is not so harmful it ought to be outlawed completely.

To reiterate: Technology provides important collective goods such as security, greatly enhanced channels of public communication, public health (e.g., by means of advances in biotechnology)—the list goes on. As such, technology has moral significance and gives rise to moral rights and responsibilities. Some of these responsibilities are, we suggest, collective responsibilities. Thus, the role occupants in law enforcement services, social media platforms, hospitals and so on have collective responsibilities to their citizens, customers, clients, patients respectively. Moreover, many of these collective moral responsibilities are also institutional responsibilities; they are responsibilities definitive of institutional roles.

4 Applying titan to regulatory problems

4.1 Cybersecurity and collective responsibility

Naturally, collective institutional responsibility is a key feature of organizational activity within and between the four groups we describe. However, there is a problem: how to understand this notion of collective institutional responsibility at the level of large organizations. Organizational action typically consists in, what Miller has elsewhere termed, *a multi-layered structure of joint actions* (Miller 2001). Obviously, given the crucial role of institutions and institutional actions in combating climate change, it is important for our purposes here that organizations that are institutions can be understood in purely individualist terms and by recourse to the core notion of joint action and, therefore in the case of morally significant joint actions, collective moral responsibility; hence the significance of the technical notion of a multi-layered structure of joint action. Note that the joint action in question could be joint epistemic action, as in the case of AI scientists developing the ChatGPT application. Importantly for our purposes here there are layered structures of joint *epistemic* action.

One relevant illustration of the notion of a multi layered structure of joint actions is a cybersecurity department comprised of three (let us assume for purposes of simplification) cyber teams: a cyber threat intelligence team (TI); an incident response team (IR), and an engineering team (EN). Suppose at an organizational level a number of joint actions ('actions') are severally necessary[3] and jointly sufficient to achieve some collective end, e.g., to prevent or mitigate malware attacks. Thus, the epistemic action of the TI team gives early warning to the IR team (which can act to prevent or, let us assume in this instance, mitigate a cyberattack) and, if necessary (as we assume it is in this instance), to the EN to enable it to 'patch' a defect in the system which the cyberattack is exploiting. Assume that the 'action' of TI is, in fact, a joint action, as is the 'action' of IR and the 'action' of EN. Moreover, assume also that the 'action' of TI, the 'action' of IR, and the 'action' of EN are severally necessary and jointly sufficient to achieve the collective end of preventing or mitigating the ongoing cyberattack, e.g., a virus; as such, these 'actions' taken together constitute a fourth joint action which is comprised of the three joint actions of TI, IR and ED (respectively).

At the first level there are individual actions directed to three distinct collective ends: the collective ends of (respectively) collecting and disseminating cyber threat intelligence, responding to the cyberattack, and removing the cyber system vulnerability. Thus, at this level there are three distinct joint actions (of TI, IR, and ED, respectively). However, taken together these three joint actions constitute a single (second level) joint action. The collective end of this single second level joint action is to mitigate the effects of the ongoing cyberattack; and from the perspective of this second level joint action, and its collective end, the three first level *joint* actions are three second level *individual* actions that are constitutive of the single second level joint action. We note that typically in organizations not just the nature, but also the quantum, of the individual contributions made to the collective end will differ from one team member to another. An army fighting a war involves a layered structure

[3] Here there is simplification for the sake of clarity. For what is said here is not strictly correct, at least in the case of many actions performed by members of organizations. Rather, typically some threshold set of actions is necessary to achieve the end; moreover, the boundaries of this set are vague.

of joint action, as does a cyber-security team (in our example). It is morally significant if it involves such actions as killing people or securing their money from theft, as is typically the case.

In fact most organizations are hierarchical institutions comprised of task-defined roles standing in authority relations to one another, and governed by a complex network of conventions, social norms, regulations, and laws. Consider a science department in a university or the forensic laboratory in a police organization: both comprise heads of department, scientists, laboratory assistants and so on, and the work of both is governed by scientific norms of observation, replication of experiments etc. Hence, most multi-layered structures of joint action, including multi-layered structures of joint epistemic action, are undertaken in institutional settings, and scientific joint epistemic action is no exception.

Notice that multi-layered structures of joint action are, as we saw in the case of joint actions, couched in purely individualist terms; they are a species of joint action. Therefore, at least in the case of morally significant joint actions performed through multi-layered structures of joint action, the participating individuals can be ascribed collective moral responsibility for the outcome of the structures and, in the case of an epistemic outcome, collective moral responsibility for the truth or, at least, probability of the truth of that outcome. However, it is not only those who produce technology through their joint activity (whether in multi-layered structures characteristic of organisations, such as corporations that have collective responsibility. The users also have responsibilities, as do legislators, regulations and others. Again, consider the responsibilities in play in relation to ensuring the collective good of *safe* transport of persons on national roads as we begin to see the rollout of autonomous vehicles. As we saw above, this relies on the contributory actions/omission of producers, users, regulators etc. It is a collective responsibility or, perhaps, a set of interconnected collective responsibilities, e.g., the collective responsibility of those involved in the design and production of the cars, the collective responsibility of legislators in the government, the collective responsibility of road users to the extent that they interact with, and have input in relation to automated technologies.

4.2 Artificial intelligence: regulatory issues and normative institutions

Artificial intelligence (AI) is already having a major positive impact on society, e.g., by enabling health professionals to more efficiently identify malignant growths or police services to deploy their limited resources to greater effect (predictive policing), and this is likely to accelerate. On the other hand, AI is already also having a major negative impact on society, e.g., by enabling disinformation on internet to be turbocharged and facilitating electoral interference by hostile foreign powers, and this is likely to accelerate. The question of how to regulate AI, is a major challenge for humanity, as it impacts on the nature of work, education, transportation, medicine, warfare, policing, government administration and many other areas. In order to address this challenge close attention needs to be paid to the mediating role that this technology has in respect of fundamental institutions and, more specifically, regulating this technology in a manner that ensures that it facilitates rather than undermines the collective goods that are the raison d'etre for these institutions. Ascribing ethically-based collective institutional responsibilities within and among some key groups of actors will be crucial. These include scientists, governments, citizens and the corporate sector. In addition, lawyers and ethicists will need to play a key role in informing government in relation to AI regulation, and educating scientists and the corporate sector on the regulatory issues, why they are important, and how they can best be addressed.

In general terms, AI refers to the application of computer systems to undertake tasks that have traditionally been performed using human intelligence. Algorithms are used to recognise patterns, perform abstract reasoning and learn from earlier examples to undertake tasks that typically involve pattern recognition. The technology is powerful and widely applicable. The most recent example is ChatGPT, an AI language model which can respond to a prompt and provide convincing written answers, having been trained on a vast amount of online text from books, encyclopedias, and academic journals. Another important and well established application of AI are autonomous vehicles that use sensors, radar and GPS to monitor the road, and environment, and navigate themselves with only limited human intervention. Algorithms control its response to the environment based on the data it receives from its sensors.

AI regulation is perhaps the most challenging of any field of technology and has a number of complexities that we can illustrate by focusing on one of the most well-developed areas of AI, is its use in the medical profession. To date, its use to diagnose images in pathology and radiology have been two contexts where it has been used most extensively, and it's likely to become more widely applied in the future. Many of the regulatory issues that have come to light in this context are representative of those that are applicable to AI more generally.

In pathology, AI assisted diagnosis can improve accuracy and efficiency, with one study finding that an AI application outperformed 11 anatomical pathologists in diagnosing breast cancer metastases (Ehteshami et al. 2017). Similarly, in radiology, the research has compared algorithms and the performance of specialist radiologists, with one study finding that an AI system outperformed six fully trained radiologists in mammogram interpretation to identify breast cancer at early stages of the disease (McKinney et al. 2020).

However, there remain a number of challenges associated with its use. For instance, it may not take account of broader information, such as the patient's clinical history and findings from a physical examination. Further, there remain issues associated with bias and error. One example from the dermatology specialty is research that found an AI system was more likely to diagnose a lesion as cancerous if the photograph included a ruler in the image, because in the images it was trained on, that was associated with a greater likelihood of cancer being present (Esteva et al 2017). There are several broader issues associated with the regulation of AI that are also relevant in medical diagnostics. For any AI system, it can be difficult to know exactly how an algorithm has arrived at a particular conclusion—this has been described as the *black box* data processing issue. As is the case in many areas where AI technology is used, clinical diagnostics can be complex and depend on a range of contextual knowledge and experience.

Human oversight, from clinicians or other relevant experts depending on the context, is crucial in maintaining accuracy and safety in relation to AI applications as their use becomes more routine over time.

The establishment of quality standards for AI algorithms in the various applications is a key aspect of improving the regulation of AI technologies. The question of which party is legally responsible for a misdiagnosis or other error of an AI algorithm may be difficult to determine and further work by regulators will also be required to provide greater certainty for those that implement and use these systems, and should be considered by regulators alongside the quality assurance question. Because AI technology is so complex, determining at what point the error occurred, and who is responsible for it, may be challenging (Smith and Heath Jeffery 2020). There are three options for liability: the party who has implemented the technology; the software company that designed the algorithm; or shared liability between these parties. In each case, it would depend on whether the party acted in accordance with standards accepted in the profession or scientific field, however, apportioning fault may be difficult due to the black box problem (Vladeck 2014).

In contrast with the most products or devices that are regulated, such as a medication or traditional car, the product is static in terms of the way it functions over time, of course some will wear down with use, but this can be measured and allowed for. An algorithm will function differently as it acquires more data and learns over time, meaning it is difficult to apply traditional models of regulation. In relation to AI diagnostics in medicine, the Food and Drug Administration is proposing a 'total product lifecycle regulatory approach' that seeks to respond this capability (FDA 2020). These complexities mean that it is crucial that collaborative approach to regulation is adopted and that it be seen as the collective responsibility of all the actors that have the necessary knowledge and expertise to ensure that society can make use of the best available technology, safely and in a way that is underpinned by appropriate regulatory frameworks. It is important to address these fundamental issues of regulation before AI has a greater role in society and increasingly takes over from humans in performing many vital functions.

The four key categories of groups we have outlined in TITAN collectively contribute to this regulatory problem and should be considered as part of a regulatory decision making framework for AI. The Producers of technology: (i) the scientists in organisational settings are collectively responsible via multi-layered structures of joint epistemic action for the development and training of algorithms, and the technology the algorithm applies, and provide fundamental information, context and evidence about the phenomenon the AI responds to, as well as correlations and modelling on the costs, benefits and impact of different interpretations and associated impacts of decisions; (ii) the technology companies produce AI integrated products, and, via multi-layered structures of joint (mainly) epistemic action are collectively responsible for the development of the technology, and are financially invested in its success. They should be incentivised and supported to transition to technologies that benefit society.

The users of technology are the ordinary citizens impacted by the technology as the consumers and beneficiaries of it. They create the market, and by purchasing products are the source of companies capital to invest in research and development. Collectively, they play a vital role in liberal democracies by electing governments with policies that effectively regulate AI. Government regulators have the capacity collectively, via multi-layered structures of joint epistemic action, to enact legislation and implement policies that regulate AI in their communities, and create incentives for private companies invest in the technology. In liberal democracies, they are elected representatives of private citizens, and their policies should reflect this mandate. Moreover, their regulation of technology should embody relevant ethical principles and should ensure that this technology facilitates rather than undermines the collective goods realised by institutions. Normative policy shapers include ethicists to provide analyses of relevant ethical concepts, including moral rights and principles but also the collective goods definitive of institutions, that are required to inform public policy and legislation. Legal professionals play a role in settling disputes within and between the above groups at national and international levels. They are necessary in order to create binding agreements between the other actors.

The interaction of these groups occurs in the context of our definition of collective goods, discussed throughout.

It is somewhat expansive in that it can potentially include aggregates of individual goods, e.g., the data from individual patients within AI diagnostic systems, or the (future) aggregate of autonomous cars relying on AI and used by most drivers on highways, thereby providing transport while also reducing car accidents. However, the definition is also somewhat restrictive in that the notion of a collective good in question is an objective notion rather than a subjective one; someone might believe something to be a good which it is not in fact, e.g., the belief that cryptocurrencies increased access to markets and could provide lucrative returns turned out to be financially ruinous for many (Lewis 2010). Moreover, collective goods in our sense are jointly produced. Thus, on our definition, the atmosphere that we need in order to breathe is not a collective good since we did not produce it. We further note that our definition of institution is somewhat expansive and includes not only those who participate narrowly in the production or maintenance of collective goods, but also those who consume or otherwise benefit from those collective goods. Consider, for instance, democratically elected governments. On our definition of such governments the citizens who vote for governments and, thereby, benefit from the collective goods provided by these governments are important elements of the democratic institutions in question. Likewise, market-based institutions on our definition include the consumers who participate as buyers in markets and consume AI and other technology-based goods and services produced.

5 Conclusion

How governments should respond to issues presented by cybersecurity and artificial intelligence technology are among the most challenging contemporary public policy issues—effective technology regulation is vital for modern society. This article has proposed a normatively informed and institutionally based account of technology regulation that contributes to addressing this issue, a Theory of Institutional Technology Actors and Norms. TITAN incorporates the perspectives of producers of technology, users of technology, government regulators of technology, and normative policy shapers; arguing that technology regulation involves a collective responsibility within and between these groups and is a matter of whether the technology in question facilitates collective good(s) produced by the relevant fundament institutions, and whether it does so in an effective, lawful and ethically sustainable manner. The theory assists by identifying the main contributors to contemporary issues in technology regulation and providing normative direction towards ethically informed legal solutions. Further work, applying TITAN to specific questions in the field will elucidate its value in understanding issues and reaching outcomes that best mediate the interests of those affected by new technologies.

Curmudgeon Corner Curmudgeon Corner is a short opinionated column on trends in technology, arts, science and society, commenting on issues of concern to the research community and wider society. Whilst the drive for super-human intelligence promotes potential benefits to wider society, it also raises deep concerns of existential risk, thereby highlighting the need for an ongoing conversation between technology and society. At the core of Curmudgeon concern is the question: What is it to be human in the age of the AI machine? -Editor.

Data availability Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

Brownsword R, Scotford E, Yeung K (eds) (2017) The Oxford handbook of law, regulation and technology. Oxford University Press, Oxford

Buitten M (2019) Towards intelligent regulation of artificial intelligence. Eur J Risk Regul 10:41–59

Ehteshami B, Veta M, van Diest P et al (2017) Diagnostic assessment of deep learning algorithms for detection of lymph node metastases in women with breast cancer. JAMA 318:2199–2210

Esteva A, Kuprel B, Novoa R et al (2017) Dermatologist-level classification of skin cancer with deep neural networks. Nature 542:115–118

Food and Drug Administration (FDA) (2020) Proposed regulatory framework for modifications to artificial intelligence/machine learning (AI/ML)-based software as a medical device. US Government, Washington

Guihot M, Matthew A, Suzor N (2017) Nudging robots: innovative solutions to regulate artificial intelligence Vanderbilt. J Entertain Technol Law 20:385–455

Habermas J (1970) Toward a rational society (J. J. Shapiro, trans.). Beacon Press, Boston

Hirvonen H (2023) Just accountability structures—a way to promote the safe use of automated decision-making in the public sector. AI Soc. https://doi.org/10.1007/s00146-023-01731-z

Johnson D, Post D (1996) Law and borders: the rise of law in cyberspace. Stanford Law Review 48:1367–1402

Lessig L (1999) Code and other laws of cyberspace. Basic Books, New York

Lewis M (2010) The big short: Inside the doomsday machine. Norton, New York

McKinney S, Sieniek M, Shetty S et al (2020) International evaluation of an AI system for breast cancer screening. Nature 577:89–94

Meckling J, Nahm J (2018) When do states disrupt industries? Electric cars and the politics of innovation. Rev Int Polit Econ 25:505–529

Miller S, Bossomaier T (2022) Cybersecurity, ethics and collective responsibility. Oxford University Press, Oxford

Miller S (2018) Dual use science and technology, ethics and weapons of mass destruction. Springer, Dordrecht

Miller S (2016) Shooting to kill: the ethics of police and military use of lethal force. Oxford University Press, New York

Miller S (2010) The moral foundations of social institutions: a philosophical study. Cambridge University Press, New York

Miller S (2015) Design for values in institutions. In: Poel I, Van den Hoven J, Vermaas P (eds) The handbook of ethics, values and technological design. Springer, Dordrecht, pp 769–781

Miller S (2017) Ignorance, technology and collective responsibility. In: Peels R (ed) Perspectives on ignorance from moral and social philosophy. Routledge, London, pp 217–237

Murray A (2007) The regulation of cyberspace: control in the online environment. Routledge, London

Murray A (2019) Information technology law. Oxford University Press, Oxford

Reed C, Murray A (2018) Rethinking the jurisprudence of cyberspace. Edward Elgar, London

Reidenberg J (1998) Lex informatica: the formulation of information policy rules through technology. Texas Law Rev 76:553–572

Smith M, Urbas G (2021) Technology law: Australian and international perspectives. Cambridge University Press, Cambridge

Smith M, Heath Jeffery R (2020) Addressing the challenges of artificial intelligence in medicine. Intern Med J 50:1278–1281

Stamper R (1977) The LEGOL 1 prototype system and language. Comput J 20:102–108

Smith M, Urbas G (2022) Evolving legal responses to social media in Australia: litigation, legislation and system architecture. ANU J Law Technol 3:8–31

Stamper R, Althaus K, Backhouse J (1988) MEASUR: method for eliciting, analysing and specifying users requirements. In: Olle T, Verrijn-Stuart A, Bhabuts L (eds) Computerised assistance during the information systems life cycle. Elsevier Science, Amsterdam

Ulnicane I et al (2020) Framing governance for a contested emerging technology: insights from AI policy. Policy Soc 40:158–177

Vladeck D (2014) Machines without principles: liability rules and artificial intelligence. Washington Law Rev 89:117–150

Wirtz B, Weyerer J, Sturm B (2020) The dark sides of artificial intelligence: an integrated ai governance framework for public administration. Int J Public Adm 43:818–829

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.