5 Ethics and border control technologies

Simone Casiraghi,* J. Peter Burgess** and Kristoffer Lidén***

* *Vrije Universiteit Brussel. E-mail: simone.casiraghi@vub.be.*

** *École Normale Supérieure, Paris & Vrije Universiteit Brussel.*
E-mail: james.peter.burgess@ens.fr.

*** *Peace Research Institute Oslo. E-mail: kristoffer@prio.org.*

5.1 Introduction

5.1.1 Definition of ethics

The two terms 'ethics' and 'morals' are sometimes used interchangeably in everyday language, but they are not synonymous. The concepts, originating from the Greek *ethos* and the Latin *mores*, respectively, both mean something like habit or custom. While the term 'morals' refers to *de facto* habits, customs and traditions, 'ethics' refers to a systematic reflection, a philosophical critique, and an evaluation thereof. Ethics is understood for the purpose of this Chapter, in the context of border control, as a synonym for moral philosophy, which is a branch of philosophy that deals, roughly, with a rational and practical reflection on what conduct is good or bad and right or wrong.

If ethics is defined as a systematic reflection on moral issues raised by emerging technologies, the purpose of this Chapter is to provide a toolkit to guide such systematic ethical reflection in the context of border control. In particular, the Chapter provides assessors with a list of recurring arguments (and recurring fallacies against which to evaluate them) that will allow them to assess the ethics component of the benchmark in the integrated impact assessment process. Thus, the structure of the Chapter is as follows: In the next sub-sections, some further introductory notions on ethics (its importance for society, historical development and literature overview) will be provided, including its importance in the assessment process and the actors involved in it. Section 5.1.2 will provide assessors with the key concepts to conduct the ethics steps of the impact assessment process accor-

DOI: 10.46944/9789461171375.5

ding to the Template included in Annex 1. The approaches that are often used at the level of applied ethics are explored, with specific examples from the context of border control. Moreover, a list of argumentative fallacies will be provided as tools through which to assess or complement these approaches.

5.1.2 The importance of ethics for society

Performing an ethics assessment involves, put simply, systematic moral reflections about how a given initiative can be 'good' and 'bad', right and wrong, or beneficial and harmful. Recent technological developments have affected every dimension of people's lives; social contacts, jobs, how they eat, travel, play, and so on. European values and moral norms have been affected in this process as well: concepts like autonomy, freedom and responsibility have been challenged and modified by the new affordances of technologies and socio-technical infrastructures.[1] For example, identity is shaped by algorithmic profiling (with systems 'predicting' people's online behaviour and purchases) and biometrics (with people's bodily parts becoming the most important identifier by which access to certain services is enabled).

More concretely, research and innovation (R&I) efforts at the European Commission (EC) in the security domain are said to contribute to tackling 'societal challenges' such as fighting crime, human trafficking and terrorism, or strengthening security through border management.[2] At the same time, the same technological developments resulting from R&I can lead to undesirable impacts on individuals and groups, distributing burdens and benefits unequally.[3] New socio-technical arrangements create genuinely new challenges, some argue, or exacerbate existing societal problems, such as systemic forms of racism and discrimination,[4] thus requiring reflection in order to identify harmful effects and take action against them.

5.1.3 The role of ethics in the benchmark

Ethics, when framed within such a definition, can be of help in an integrated impact assessment process, not as an alternative to a legal assessment based on fundamental rights, but rather as an argumentative support. The scope of this Chapter is therefore the integration of ethics of technology into the impact assessment process, with the intention of introducing a 'how to' method to assessing the uses and implementations of new and emerging border technologies. The ethical component of the impact assessment method is meant to support and/or expand upon the data protection component, which constitutes the 'backbone' of such a method.[5] This especially means that, besides the necessity and proportionality assessment and risk assessment that are mandated by law as part of a Data Protection Impact Assessment (DPIA),[6] the integrated impact assessment method adds an 'ethics assessment' to the appraisal techniques, in order to further expand on the assessment of the risks to rights and freedoms of natural persons. Such an expansion gives assessors a broader political and societal view on the impacts of border control technologies in addition to individual data protection issues[7] by also looking at arguments relating to the values these technologies aim to uphold, their (supposed) neutrality, or the unequal distribution of burdens and benefits among groups of people.

However, assessors need to pay attention to the use of the term 'ethics' when it comes to assessing the impacts of emerging technologies. On the one hand, ethics is currently an inflated term or buzzword, used with different meanings depending on the interests at stake for specific groups. Reference to ethics can be made by academics, humanitarian or non-governmental organisations, civil society representatives, technology companies (e.g. the ethical principles of Google or Microsoft) or political institutions (such as the European Commission), with each pursuing possibly different – and even competing – goals. On the other hand, both academics and civil society organisations[8] have warned about the excessive use of 'AI (Artificial Intelligence) ethics' which could become an obstacle to traditional regulation, and a way of self-legitimising industry practices.[9] Given the proliferation of ethics principles, guidelines and methods in recent years,[10] assessors may be provided with tools that can guide them throughout the assessment process and, more generally, can consider the current debates, without the risk of considering ethics an empty signifier. Before turning specifically to the approach of the integrated impact assessment method, however, it is useful to quickly look at the historical development of applied ethics and ethics assessment tools.

5.1.4 Historical development of applied ethics

The historical roots of the word 'ethics', as part of a philosophical enterprise, can be traced back to Ancient Greece, to the work of Plato and Aristotle in the 5th and 4th centuries BCE, among others. In the West, ethics remained for centuries predominantly a matter limited to philosophical discussion.[11]

Until recently, then, ethics primarily had an academic and theoretical role. In the second half of the 20th century, however, ethics, first and foremost in the form of bioethics, began to acquire a political and institutionalised role.[12] The main explanation that is often given for this political turn is the increased risks associated with research on human subjects through biotechnical medicine. However, this explanation is overly simplistic.[13] An additional explanation is that the rise of institutionalised ethics reflected the need to establish a more open dialogue between science and society.[14] Since the 1970s, the EU has sought to strike a balance between facilitating and promoting science on the one hand and respect for the pluralism of European values on the other, as a response to value conflicts in areas including medicine and food and agriculture.[15]

Following bioethics, computer ethics, environmental ethics, and, more recently, robo-ethics, big data ethics and AI ethics proliferated as forms of 'applied ethics', i.e. forms meant to address specific challenges in different domains by applying rigorous philosophical reasoning in an attempt to solve moral dilemmas or guide decision-making. Applied ethics involves an inter-disciplinary discussion, often outside academia, and related to policy making and decision-making processes in private (e.g. companies) or public institutions (e.g. research committees or advisory bodies).

Among the methods for performing applied ethics, ethical technology assessment and ethical impact assessment have emerged as new anticipatory methods (i.e. techniques of anticipatory governance to tackle impact of technologies *before* they materialise), as well as approaches such as Responsible Research and Innovation (RRI),[16] to combine the more strategic and technical dimension of R&I with the more normative one of responsibility.[17] Such anticipatory and responsible approaches have opened up the topic of 'ethics' to a multi-disciplinary arena of actors, instead of keeping it confined to the realms of philosophers or academics.

5.1.5 The profile for assessing ethics

Today, the landscape of applied ethics is multifaceted. Compliance with ethics requirements, depending on the initiative, may be assessed by a variety of bodies such as:

- Research Ethics Committees (RECs), at public (e.g. universities) or private (e.g. companies) organisations, which calculate the risks and benefits of a given initiative and ensure participants give informed consent,[18]
- National ethics committees or councils,[19] at EU or Member State level, or
- Groups of ethics experts recruited in an *ad hoc* manner.[20]

An integrated impact assessment process, however, requires a team of assessors that works together across several domains. Looking at the composition of ethics committees and ethics advisory boards, members may be drawn from medicine, business, engineering, computer science, or elsewhere, depending on the field to which ethics is applied. It is therefore a challenge to identify the profile required to perform the ethics steps of the integrated impact assessment process.

There are no clear-cut solutions to this challenge. Moreover, giving a definitive answer to these questions would risk making 'ethics' a type of expertise inaccessible to some profiles. Instead, engaging in ethical discussions is, and should be, open to different profiles, provided that assessors are open to critical thinking (including in their own daily activities) and willing to familiarise themselves with the key concepts provided in Section 5.2. In any case, assessors with a background in humanities, and more particularly in philosophy (specialised in philosophy of technology, applied ethics, RRI), social sciences (specialised in surveillance studies, critical security studies or science and technology studies) or law and technology (including criminology), might need less effort to acquaint themselves with the approach described here.

If in the team of assessors there are no persons able to carry out this part of the assessment process, or it is not possible to hire extra personnel to carry out the assessment, this could mean two main things. First, it would provide an opportunity for personnel of the institution in charge of the assessment to be encouraged to acquire new expertise through, for example, training. Alternatively, it may offer a chance to open up the assessment process to stakeholder involvement, for example through the team of assessors organising events or sessions with external experts or members of the public who can provide relevant input or support.

5.1.6 Literature overview

Despite recent tendencies of coupling and blurring ethical and legal considerations of technologies in areas such as security research,[21] ethics and law are better understood as distinct, with each having its own questions and approaches.[22] This separation is reflected in the benchmark of the integrated impact assessment process. The interdisciplinarity of ethics, however, coupled with the fact that there is no specific 'ethics of border control technologies', (as there are, for example, bioethics, business ethics and computer ethics as established forms of applied ethics),[23] might confuse assessors when it comes to choosing instruments (texts, methods, techniques) to support the assessment process. However, there are at least two groups of sources that could provide support to assessors. These are:

A. Generic anticipatory or assessment methods that can be applied to the case of ethics of border control. A plethora of methods by which to undertake ethics in R&I exist, but the main groups can be classified in:[24]
    - *Ex-ante* methods, i.e. aiming at addressing ethical issues at an early stage of the R&I process, such as Ethical Technology Assessment,[25] Pragmatist New and Emerging Science and Technology (NEST) ethics,[26] or scenario approaches;[27]
    - Intra methods, taking place at the design or testing phase, like Value-Sensitive Design,[28] ethical impact assessment, or mediation theory;[29] or
    - *Ex-post* methods, i.e. those performed on concrete applications of already-finished R&I processes, like checklist approaches or principle-based ethics.[30]

B. Texts by scholars and activists[31] who address issues of surveillance and management of 'smart border' solutions,[32] which can help assessors to identify recurring arguments in the assessment process. In particular, the following are to be considered recurring challenges:[33]
    - Reduction of dynamic and biographical identity of travellers to static biological samples;[34]
    - Creation of 'technologies of power', which enable institutions to control citizens and exploit their bodies; a dark side to the promise of more efficient and objective identification practices;[35]
    - Excessive economic costs of border control technologies in comparison to the advantages they bring, such as high maintenance costs, technical seatbacks, or difficulty in adjusting to regulations;[36]

- Increased chances of vulnerabilities such as hacking, identity theft and manipulation of data;[37]
- Risks of discrimination and replication of racial prejudices, especially concerning the treatment of citizens from third countries, who often need to undergo extra checks and, depending on their ethnicity or social background, might be more readily associated with terrorism or smuggling.[38]

5.2 Ethical arguments and fallacies

5.2.1 Ethics and technology arguments

This Section presents a list of ethical arguments that assessors need to identify, analyse and assess.[39] The list includes the most recurrent arguments (and related counter-arguments) that are prevalent in the literature and in public debates on border control technologies. Engaging with ethical arguments is not a standalone exercise, but an argumentative support to the legal and social acceptance aspects of the integrated impact assessment process.

Universality of principles and/or values: A technology is developed on the basis of values or principles that are assumed to be universal. The idea is that there is a set of 'core' of principles that are applicable, or values that are shared, across cultures.[40] In turn, from these values, one can 'deduct', *a priori*, a core number of universal principles (4 in the case of bioethics) that are applicable in any practice. The same arguments are replicated today in the fields of Artificial Intelligence (AI)[41] and biometrics,[42] both of which that have been utilised in border control. Opponents of this argument stress that people might disagree on what values or principles count. In this case, values or principles might apply only to a specific situation (or culture, or even technological context), but not to another. A bigger problem is that principles and values might be dictated or decided upon by those who are already in power, and later 'exported' to other (more specifically, more vulnerable or less powerful) people, under the alleged assumption of universality.

Technological determinism: A technology will *inevitably* bring about some positive or negative effects. This argument can take optimist or pessimist forms. Technology optimists argue in favour of technological developments as a panacea for long-lasting social problems. Almost any form of technological progress will bring about some social progress, including in the context of border control. Biometrics and smart borders, for instance, are often seen as a 'silver bullet' for identification: they are portrayed as more reliable, accurate and efficient than traditional means of identifying people. They can 'solve' problems of airport security (by identifying potential threats) or migration flows (by speeding-up border checks). Technology pessimists instead insist on the negative effects of technologisation, often with nostalgic tones. Technology is a form of alienation, and a deterministic force than cannot be stopped. It makes humans interchangeable forces, and takes away their individualism. One form of alienation in border control stems from the massive use of biometric systems. A rich and dynamic identity of a person, which includes their personal story, interests or personality, is flattened over their static bodily identity, represented by a digital token (e.g. a fingerprint, facial image or retinal scan).[43]

Neutrality of technology: *Per se*, technology is neutral, that is, it is neither beneficial nor harmful: it depends on the use that is made of it to achieve a certain goal. An example is Live Facial Recognition (LFR)[44] deployed by some national law enforcement authorities, such as the London Metropolitan Police (UK), the police in Hamburg and Berlin (Germany) and in Nice (France).[45] Some would claim LFR is neutral: it can be used responsibly to make public spaces safer, by preventing and investigating criminal offences, but it can also be misused, e.g. when its use is not strictly necessary or it has detrimental effects on a person that is wrongly identified as a criminal.[46] However, many oppose this neutrality thesis as too simplistic. Technological artefacts cannot be considered in isolation, but always as parts of social worlds. In other words, there are no such things as technological artefacts in and of themselves, but they always mediate and are mediated by society.[47] For example, programmers already project (willingly or not) certain possible uses, values or biases upon a technology, for example, amplifying racial hierarchies.[48] Consequently, technologies could have unforeseen effects or uses that were not considered at the design phase, or that are not strictly related to the original goal. For instance, higher rates of misidentification by LFR algorithms could lead to disproportionate interference with certain ethnic groups, e.g. through unnecessary police stops and requests to show proof of identity.[49]

Arguments from precedence: New technologies are not really 'new', but rather they re-propose the same benefits and challenges of older ones. In the case of border control technologies, in a positive sense, an analogy is often made between biometric and non-biometric passports or identity documents. Identity documents have existed for a long time, and people have become accustomed to them; biometric documents do not pose additional problems (they are still vulnerable to, for example, theft and falsification); therefore, one should not worry about identity documents that include biometric features.[50] Opponents of the argument of precedent claim that the changes of emerging technologies are so disruptive, rapid and large-scale that the analogy with precedent technologies no longer holds.[51] Since biometric systems might collect a huge amount of data, combine different types of biometric samples (e.g. fingerprint, retina, gait, voice, etc.) and store them in possibly interoperable databases, the purpose(s) of which might not be clearly defined in advance, they are worthy of greater attention.

Change of ethical values: Technologies change our values, leading to moral progress or moral decline.[52] Some argue that technologies help people to progress ethically, e.g. to take better decisions in ethical dilemmas, act according to higher ethical standards, or better discern values and principles at stake. This happens both at an individual and a societal level. For example, in the context of border control, biometric identification techniques could be seen as enhancing the impartiality of border checks. The process of recognition is carried out by automated systems, thus boosting the fairness of the outcomes. The idea is that, while people can have biases, automated machines do not, and are consequently more equitable. Newer verification systems based on a combination of biometric traits are also seen to outperform the current limitations of other automated biometrics, such as fingerprinting, in terms of neutrality and reliability. Opponents of the argument of ethical progress stress instead how, despite cases of progress in recent years, ethical decline has also taken place. Considering something to be ‘progress’ is highly dependent upon a specific point of view: what counts as progress for one person might not for another. Technological developments often increase inequalities between areas of the world and groups within society, enhancing the welfare of the Western countries at the expense of the Global South, or making big companies richer at the expense of unaware customers.[53] Moreover, machines and algorithms are designed by humans, and as such they can embody prejudices and biases subconsciously introduced by their programmers.[54]

Slippery slope: Using a metaphor, once one makes the first steps on the slope, it becomes impossible to stop until bad consequences happen. In relation to technology, the idea is that some relatively innocuous or small-scale technological developments could bring about, if developed on a large scale, a cascade of uncontrollable and unpredicted negative effects.[55] Alternatively, technology supporters might claim that if a new technology is not implemented now, people will suffer all types of terrible consequences. Opponents of this argument say that people are able to escalate easy generalisations from one specific case to multiple ones; that there is no convincing evidence that simply allowing some exceptions to moral rules will bring about a collapse of the whole system of rules; finally, that the possibility of exceptions does not necessarily mean that these exceptions will also occur on a larger scale.

‘*Function creep*’: In short, function creep means the use of a specific initiative (e.g. a border control technology) for a purpose for which it was not originally intended.[56] With reference to biometric technologies, storing biometric data in a central database might permit that such data are (re-)used for purposes not initially foreseen, like profiling or criminal investigations. An example is when Europol and law enforcement agencies were granted access to the information stored in the Visa Information System (VIS) for detection and investigation of terrorist offences.[57] This is not in line with the original purpose of the system,[58] which was established in 2004[59] to improve the management of a common EU visa policy and to enhance the security of visas. However, in 2008, when the Regulation for the VIS was adopted,[60] access was granted under certain circumstances, a purpose that was not foreseen when the system was established in 2004.[61]

5.2.2 Normative ethics

A specific subset of ethical arguments is related to normative ethical positions. Roughly, the crux of this issue is which specific ethical rules should govern conduct. This Section follows a tripartition between deontological, consequentialist and distributive justice arguments.[62]

Deontological arguments define rules on the basis of fundamental moral principles. An action is considered to be 'morally right' if it conforms to certain principles, rights, duties, prohibitions, or responsibilities, and/or if the actor has certain intentions, regardless of the consequences of such action. Roughly speaking, the definition of duty precedes that of what counts as 'good'.[63] Deontological arguments can be also weaker (admitting exceptions or performing balancing between principles or duties) or stronger (requiring moral integrity and no exception, with certain actions being categorically prohibited). The main examples of deontological arguments in the technological domain are drawn from principle-based ethics, human rights and codes of professional conduct.

- In principle-based ethics, principles are abstract action guides (*do x*), but sometimes they can also categorically prohibit a certain action (*don't do y*). As a concrete example, the High-Level Expert Group on AI defines their principles as 'ethical imperatives' that AI practitioners should *always* strive to adhere to.[64]
- In human rights ethics, human rights are moral entitlements that any person has and that have to be considered before the consequences. Sometimes, fundamental rights enshrined in legal texts[65] are also taken as foundations of ethical principles in the public discourse, such as in the EU's debates on privacy and new technologies.[66]
- In codes of professional conduct, sets of rules or principles exist that should guide the conduct of practitioners when exercising their profession. Codes of conduct can be written by companies, but also by professional associations. One of the earliest expressions of professional ethics is the Hippocratic Oath, which has been used in the medical profession for centuries. Examples of codes of conduct can also be found in border control.[67]

The main shortcomings of deontological rules are that they are often difficult to live up to, they require a strong commitment, and they admit few-to-no exceptions. Also, there is often a gap between abstract principles and more concrete situations, which makes it difficult to apply the principles. To overcome the rigidity of deontology and its vagueness in guiding action, consequentialist arguments are often offered as alternatives.

Consequentialist arguments (among which: utilitarian) state that actions are right or wrong only on the basis of their outcomes (i.e. consequences). In other words, among the possible actions available, one chooses the option that maximises the expected outcomes (or degree of utility).[68] Thus, contrary to deontology, there are no *a priori* wrong acts (e.g. murder) and an act is right whenever it is the one that produces the best possible consequences relative to any other. Consequentialist arguments can take many forms, depending on how the consequences or degree of utility are quantified: for example, in terms of pleasure, satisfaction of preferences or economic factor.[69] Consequentialist arguments fit well with risk-based approaches and cost-benefit analyses precisely because they offer more quantitative, calculable ways to solve moral dilemmas.

To recognise a consequentialist argument, a rule-of-thumb could be to look at whether a trade-off is proposed. A classic trade-off in border control discourses is that of security versus privacy: surveillance technologies require the giving away of some privacy (e.g. by allowing the processing of one's sensitive data and sharing them with third parties) in exchange for extra security (e.g. less risk of identity theft, less risk of dangerous people entering a plane).

Trade-off discourses can be criticised for being overly simplistic: problems that are presented as mathematical, quantifiable and objective are in fact value-laden. The risk of these discourses is that political conflicts and power asymmetries are reframed as mere technical ones.[70] For example, it could be shown how, in a specific case (say, the introduction of a system of new-generation cameras at an airport), privacy and security *should not* be understood as an abstract trade-off, that can simply be solved by using metrics that assign a numeric value to privacy and another to security. The language of trade-off[71] is often enforced in contexts (cultures, organisations) that systematically favour security (e.g. to defend travellers from terrorist attacks), while both privacy and security could be enforced without losses for either of the two.[72] Another criticism is that consequences are often uncertain and not easy to predict, especially when it comes to emerging technologies. A classic example is environmental consequences of technologies, for instance how the use of cars has increased pollution in cities. Finally, consequentialism fails to take seriously the distinction between persons,[73] since what counts is the aggregate results of consequences, also at the cost of serious damages for small groups of people, like minorities. This is a problem in border control, where technologies are often beneficial for large groups of people (*bona-fide* travellers) but can be unavailable or detrimental for smaller groups (third country nationals, high-risk categories, or refugees).

Distributive justice arguments[74] state that an action is deemed morally problematic whenever some benefit to which a person is entitled is denied (without any compelling reason) or whenever there is an unequal distribution of benefits and burdens.

Justice arguments can take a more positive or negative stance. In a positive sense, it can be admitted that, at first, the distribution of a new technology is not proportionate. It is inevitable that a small amount of people could initially benefit from it, but eventually everyone will profit from it. A small group 'paves the way' for the more large-scale use of technology. In a negative sense, the same biometric features and identification technologies that are used can be indeed quite convenient and efficient for some, but they are also used to restrict the movement of others by those who are in power.[75] This could lead, on the one hand to the reinforcement of privileges of some groups (like EU and US citizens) and, on the other, to the increased discrimination against other groups (like asylum seekers). An example of this is the old Fast Low Risk Universal Crossing (FLUX Alliance) traveller program for US and Dutch frequent intercontinental travellers, which is based on biometric identifiers including fingerprints and retinal imaging.[76] So-called 'low risk passengers', i.e. with no criminal records, customs or immigration conviction, can apply for the program. If the interview and security threat assessment is successful, they can have, at the cost of paying an additional fee, the advantage of skipping queues and border checks.

5.2.3 Types of ethical fallacies

As shown in the previous Sections, ethical arguments can always be criticised. One way of showing that an argument is not convincing is to demonstrate a deficit in the structure of the argument (also known as a logical fallacy). A fallacious argument is a reasoning that seems convincing at first, but is based on weak assumptions, and/or the conclusions do not follow from the premises. The list of fallacies provided here is tailored down to ethical arguments relevant for the context of border control, which are therefore referred to as 'ethical' fallacies. The list could give assessors some critical tools to challenge what is usually taken for granted or under-emphasised in public discourse.

The list below is not exhaustive, but was selected on the basis of application to the arguments outlined in Section 5.2.[77] Taking inspiration from this list, assessors could expand the list of fallacies for their assessments.

Begging the question, or *petitio principii*: These are arguments that include in their premises the argument they aim to demonstrate. Such an argument is technically valid, but useless in demonstrating its conclusions. A classic example could be this: 'The technology is ethical because it is compliant with ethical principles'. In this example, the conclusion (i.e. the fact that a technology is ethical) does not add anything new to the premises (the fact that the technology complies with ethical principles).

Ad hominem: An argument is refuted on the basis of the person (or company or institution) that is proposing the argument. This argument is fallacious because it should focus on the merit of the argument (validity of premises, line of reasoning, clarity of exposition) and not on some (possibly irrelevant) qualities of the proposer. An example could be that 'The ethics principles endorsed by Person X are unreliable because Person X is known for not respecting such principles in their private life'. The argument can be fallacious, *if* it is not based on content or process to draw the principles endorsed by Person X, but *only* on the bad name that Person X bears in public discourse.

Appeal to a (moral) authority, or ipse dixit: This is an argument where the opinion of an authority is used as irrefutable evidence to support the argument. For example, it can be said that 'A technology is ethical because X said that' or that 'A technology is ethical because it is compliant with the principle issued by X'. Reference to 'moral' authorities is not warranted here, since it is not clear who has established that an author or ethical advisory body is an authority, why they cannot be wrong, or whether the people who decided on the principle were democratically elected or chosen to do so. The argument is fallacious because the soundness of the opinions of the authority are taken for granted and not questioned.

Confusion of ethics and law: In these arguments, the boundary between the law and ethics is blurred. This can happen in both directions. 'If a technology is legal, then it is ethical' is fallacious, because the legal compliance of a technology does not automatically make it morally acceptable. But also, the converse is problematic 'if a technology is ethical, then it must be legal'. This is questionable when it is consistently argued that 'the law lags behind' and cannot maintain the pace of technological development; therefore, ethics is needed to go 'beyond the law'.[78] If ethics is not properly defined, and ethics principles are arbitrarily constructed, they may be in contrast with the law (e.g. with fundamental rights).

Naturalistic fallacy: These arguments are characterised by the unwarranted deduction of prescriptions (*X should* …) from descriptions (*X is* …). Simply put, if something took place a number of times, it *must* be true: 'If a country is implementing measures to deploy interoperable large-scale databases, then people should accept them'. This is fallacious because a normative conclusion (people *should* …) is derived from descriptive premises (a country *is* implementing …). To be sound, the argument needs to have both conclusions and premises either in the descriptive or prescriptive form.

Ambiguity: A key word can assume multiple meanings. Usually, the correct meaning is deduced from the context, but when this is not the case, an argument can take different meanings, thus becoming weaker. An example is the use of the word 'ethics' as a subject of a sentence ('ethics can help to', 'ethics can contribute to', 'ethics can clarify', etc.). For example: 'Ethics will help the border guards to identify the risk of the biometric technology'. In this case, ethics can mean, for example, a specific training, a textbook, a set of arguments, or a group of ethics experts. But the problem is that it is unclear what type of ethics people are talking about, what type of ethics experts are involved, or who selected these. If this is not specified, the argument loses its force and can be misused.

Privacy fallacy: 'If you haven't done anything wrong, you have nothing to hide'. This argument is fallacious on many levels. First, not *only* do people that did something wrong need to be protected by privacy. Being exposed can carry risks, regardless of the fact that one has something to hide. For example, people might be discriminated against by banks, insurers or employers if their health records are made public. Second, one might not have done anything wrong, but still, due to a failure of the system, be found guilty or wrongly stigmatised as a criminal, only because they belong to a certain ethnic group.

Appeal to emotion: These are arguments that appeal to the subject's emotion in order to encourage them to accept arguments whose premises are weak or dubious. One example could be appeal to fear of anxiety of 'external threats', like the need to develop invasive technologies against the menace of terrorism, in spite of the majority of terrorist attacks in Europe resulting from actions of internal 'residual terrorists' (e.g. far-right groups or separatists) and not of international groups.[79]

Technocratic fallacy: These arguments take the form of 'It is an engineering issue how X is dangerous; therefore, engineers should decide whether X is acceptable'.[80] 'Dangerous' could also be changed to 'secure', 'privacy-friendly', and so on. The argument is fallacious because engineers (or other experts) may be competent in deciding how X is dangerous, but not the extent to which it is morally acceptable.

False analogy: These are arguments that use analogical reasoning; since something is morally accepted/acceptable in a certain case, then is *must* be accepted in a similar case, too. For instance, 'Since biometric technologies have been accepted in criminal investigations for their accuracy, then they must be used in everyday life too'. Arguments like this could be fallacious because the properties used to make the analogy are not relevant to drawing the conclusions. The reasons that make biometrics acceptable in criminal investigations are not the same as those that (would) make them acceptable in public life.

Endnotes

1. European Data Protection Supervisor Ethics Advisory Group, "Towards a Digital Ethics," 2018.
2. See Annex I Part III of Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC, OJ L 347, 20.12.2013, p. 104–173.
3. Zach Campbell, Caitlin L Chandler, and Chris Jones, "Sci-Fi Surveillance: Europe's Secretive Push into Biometric Technology," *The Guardian*, 2020.
4. Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Cambridge, UK: Polity Press, 2019); Petra Molnar, EDRi, and the Refugee Law Lab, "Technological Testing Grounds. Migration Management Experiments and Reflections from the Ground Up," 2020.
5. Dariusz Kloza et al., "Data Protection Impact Assessment in the European Union: Developing a Template for a Report from the Assessment Process," d.pia.lab Policy Brief (Brussels: VUB, 2020), https://doi.org/10.31228/osf.io/7qrfp.
6. See Chapter 4 in this Volume.
7. Nina Boy, Elida Jacobsen, and Kristoffer Lidén, "Societal Ethics and Biometric Technology," PRIO (2018), https://www.prio.org/utility/DownloadFile.ashx?id=1708&type=publicationfile.
8. See: https://edri.org/our-work/attention-eu-regulators-we-need-more-than-ai-ethics-to-keep-us-safe/.
9. Paul Nemitz, "Constitutional Democracy and Technology in the Age of Artificial Intelligence," *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 376, no. 2133 (2018): 1–25, https://doi.org/10.1098/rsta.2018.0089; Ben Wagner, "Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?," in *Being Profiled. Cogitas Ergo Sum*, ed. Mireille Hildebrandt (Amsterdam: Amsterdam University Press, 2018), 84–89; Karen Yeung, Andrew Howes, and Ganna Pogrebna, "Why Industry Self-Regulation Will Not Deliver 'Ethical AI': A Call for Legally Mandated Techniques of 'Human Rights by Design,'" in *The Oxford Handbook of Ethics of AI*, ed. Markus D. Dubber, Frank Pasquale, and Sunit Das (Oxford, UK: Oxford University Press, 2020).
10. Niels van Dijk and Simone Casiraghi, "The 'Ethification' of Privacy and Data Protection in the European Union. The Case of Artificial Intelligence," *Brussels Privacy Hub Working Paper*, 6, 2020.
11. It is impossible to give a comprehensive account of the history of ethics intended as moral philosophy in the present Chapter. For an overview, see Alasdair MacIntyre, *A Short History of Ethics. A History of Moral Philosophy from the Homeric Age to the Twentieth Century* (Notre Dame, Indiana: University of Notre Dame Press, 1998).
12. Alan Petersen, *The Politics of Bioethics* (London: Routledge, 2011); Ulrike Felt et al., *Taking European Knowledge Society Seriously*, Office for Official Publications of the European Communities (Luxembourg, 2007).
13. Felt et al.

14. Nancy S. Jecker, Albert R. Jonsen, and Robert A. Pearlman, *Bioethics. An Introduction to the History, Methods and Practice* (Sudbury, MA: Jones and Bartlett Publishers, 1997).
15. Examples are the 'mad cow' crisis or the transatlantic trade wars over hormone-treated beef in the 1990s. Sheila Jasanoff, *Designs on Nature. Science and Democracy in Europe and the United States* (Princeton, New Jersey: Princeton University Press, 2007).
16. RRI became increasingly important in the years around 2010, especially in the EU's Framework Programme Horizon 2020. Rene Von Schomberg, "A Vision of Responsible Research and Innovation," in *Responsible Innovation. Managing the Responsible Emergenve of Science and Innovation in Society* (Wiley, 2013), 51–74.
17. Robert Gianni, John Pearson, and Bernard Reber, eds., *Responsible Research and Innovation. From Concepts to Practices*, *Responsible Research and Innovation* (London & New York: Routledge, 2018), https://doi.org/10.4324/9781315457291.
18. Allison Ross and Nafsika Athanassoulis, "The Role of Research Ethics Committees in Making Decisions about Risk," *HEC Forum : An Interdisciplinary Journal on Hospitals' Ethical and Legal Issues* 26, no. 3 (2014): 203–24, https://doi.org/10.1007/s10730-014-9244-6.
19. The most well-established are often specialised in health and life sciences, such as *Der Duetsche Ethikrat* in Germany (see https://www.ethikrat.org/en/the-german-ethics-council/) or the *Comité, Consultatif National d'Éthique* in France (see https://www.ccne-ethique.fr/en).
20. For example, the ethics review process of an EU-funded research proposal. For a description of the process in the security domain, see Matthias Leese, Kristoffer Lidén, and Blagovesta Nikolova, "Putting Critique to Work. Ethics in EU Security Research," *Security Dialogue* 50, no. 1 (2018): 59–76.
21. Examples are also Ethical, Social and Legal Implications (ELSI) of emerging technologies in the United States (Michael S Yesley, "What's ELSI Got to Do with It? Bioethics and the Human Genome Project," *New Genetics and Society* 27, no. 1 (2008): 1–6, https://doi.org/10.1080/14636770701843527), mostly related to genomics and nanotechnology, and Responsible Research and Innovation (RRI) in the EU (Gianni, Pearson, and Reber, *Responsible Research and Innovation. From Concepts to Practices*).
22. Gloria González Fuster and Serge Gutwirth, "Ethics, Law and Privacy. Disentangling Law from Ethics in Privacy Discourse", *Proceedings of the 2014 IEEE International Symposium on Ethics in Science, Technology and Engineering* (2014).
23. With relative curricula, courses, dedicated conference and journals, and so on.
24. Wessel Reijers et al., "Methods for Practising Ethics in Research and Innovation: A Literature Review, Critical Analysis and Recommendations," *Science and Engineering Ethics* 24, no. 5 (2018): 1437–81, https://doi.org/10.1007/s11948-017-9961-8.
25. Elin Palm and Sven Ove Hansson, "The Case for Ethical Technology Assessment (ETA)," *Technological Forecasting and Social Change* 73, no. 5 (2006): 543–58, https://doi.org/10.1016/j.techfore.2005.06.002; Asle H. Kiran, Nelly Oudshoorn, and Peter Paul Verbeek, "Beyond Checklists: Toward an Ethical-Constructive Technology Assessment," *Journal of Responsible Innovation* 2, no. 1 (2015): 5–19, https://doi.org/10.1080/23299460.2014.992769.
26. Tsjalling Swierstra and Arie Rip, "Nano-Ethics as NEST-Ethics: Patterns of Moral Argumentation about New and Emerging Science and Technology," *NanoEthics* 1, no. 1 (2007): 3–20, https://doi.org/10.1007/s11569-007-0005-8.
27. Gill Ringland, "The Role of Scenarios in Strategic Foresight," *Technological Forecasting and Social Change* 77, no. 9 (2010): 1493–98, https://doi.org/10.1016/j.techfore.2010.06.010.
28. Batya Friedman, Peter Kahn, and Alan Borning, *Value Sensitive Design: Theory and Methods* (University of Washington Technical, 2002), https://faculty.washington.edu/pkahn/articles/vsd-theory-methods-tr.pdf.

29. Ibo van de Poel et al., *Ethics, Technology and Engineering: An Introduction* (Wiley Blackwell, 2011). Peter-Paul Verbeek, *What Things Do. Philosophical Reflections on Technology, Agency and Design* (Pennsylvania State University Press, 2005).
30. High-Level Expert Group on Artificial Intelligence, "The Assessment List for Trustworthy Artificial Intelligence," 2020.
31. These authors do not necessarily call themselves 'ethics experts' or 'ethicists', but their inputs are relevant for the benchmark in this Chapter.
32. The EU's 'smart borders' are automated systems to speed up and facilitate the border check procedure of the majority of travellers, and specifically (but not exclusively) to hinder and stop those migrants that pose a threat to the security of the Union through their status of irregular migrants, criminals or terrorists. See: European Commission, "Stronger and Smarter Information Systems for Borders and Security", COM/2016/0205 final.
33. These challenges are further expanded in the Section 5.2.
34. Katja Franko Aas, "'The Body Does Not Lie': Identity, Risk and Trust in Technoculture," *Crime, Media, Culture* 2, no. 2 (2006): 143–58, https://doi.org/10.1177/1741659006065401; Katja Franko Aas, "'Crimmigrant' Bodies and Bona Fide Travelers: Surveillance, Citizenship and Global Governance," *Theoretical Criminology* 15, no. 3 (2011): 331–46, https://doi.org/10.1177/1362480610396643; Btihaj Ajana, "Recombinant Identities: Biometrics and Narrative Bioethics," *Journal of Bioethical Inquiry* 7, no. 2 (2010): 237–58, https://doi.org/10.1007/s11673-010-9228-4; David Lyon, *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination*, *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (London & New York: Routledge, 2005), https://doi.org/10.4324/9780203994887.
35. Chris Jones, "Automated Suspicion: The EU's New Travel Surveillance Initiatives," 2020; Chris Jones, Jane Kilpatrick, and Mariana Gkliati, "Deportation Union: Rights, Accountability, and the EU's Push to Increased Forced Removals," 2020.
36. Julien Jeandesboz, "Smartening Border Security in the European Union: An Associational Inquiry," *Security Dialogue* 47, no. 4 (2016): 292–309, https://doi.org/10.1177/0967010616650226.
37. Pinja Lehtonen and Pami Aalto, "Smart and Secure Borders through Automated Border Control Systems in the EU? The Views of Political Stakeholders in the Member States," *European Security* 26, no. 2 (2017): 207–25, https://doi.org/10.1080/09662839.2016.1276057.
38. Matthias Leese, "The New Profiling: Algorithms, Black Boxes, and the Failure of Anti-Discriminatory Safeguards in the European Union," *Security Dialogue* 45, no. 5 (2014): 494–511, https://doi.org/10.1177/0967010614544204.
39. The way in which these recurring arguments are presented is inspired by NEST ethics as presented in Tsjalling Swierstra, "Introduction to the Ethics of New and Emerging Science and Technology," in *Handbook of Digital Games and Entertainment Technologies*, 2015, https://doi.org/10.1007/978-981-4560-52-8_33-1; Swierstra and Rip, "Nano-Ethics as NEST-Ethics: Patterns of Moral Argumentation about New and Emerging Science and Technology."
40. Tom L. Beauchamp, "Common Morality, Human Rights, and Multiculturalism in Japanese and American Bioethics," *Journal of Practical Ethics* 3, no. 2 (2015): 18–35.
41. High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI," 2019.
42. For example, the ethics principles published by the Biometrics Institute, a multi-stakeholder international community, at: https://www.biometricsinstitute.org/ethical-principles-for-biometrics/.
43. Ajana, "Recombinant Identities: Biometrics and Narrative Bioethics."
44. See Chapter 6 in this Volume.
45. European Union Agency for Fundamental Rights, "Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement," 2019.

46. Pete Fussey and Daragh Murray, 'Independet Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology' 128, 43, http://repository.essex.ac.uk/24946/.
47. Verbeek, *What Things Do. Philosophical Reflections on Technology, Agency and Design*.
48. Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*.
49. Silkie Carlo, Jennifer Krueckeberg, and Griff Ferris, "Face Off: The Lawless Growth of Facial Recognition in UK Policing," *Big Brother Watch* (2018): 56.
50. For a critique of this argument, see Simone Casiraghi, 'Should (Your) Identity Documents Use Biometrics?' (2018), https://www.eticasconsulting.com/wp-content/uploads/2018/04/Origins_-FINAL.pdf.
51. Julian Savulescu, Ruud ter Meulen, and Guy Kahane, eds., *Enhancing Human Capacities* (Oxford, UK: Wiley-Blackwell, 2011).
52. Hanno Sauer, "Butchering Benevolence Moral Progress beyond the Expanding Circle," *Ethical Theory and Moral Practice*, 2019, https://doi.org/10.1007/s10677-019-09983-9.
53. Christian Fuchs, "The Political Economy of Privacy on Facebook," *Television and New Media* 13, no. 2 (2012): 139–59, https://doi.org/10.1177/1527476411415699.
54. Kevin Macnish, "Unblinking Eyes: The Ethics of Automating Surveillance," *Ethics and Information Technology* 14, no. 2 (2012): 151–67, https://doi.org/10.1007/s10676-012-9291-0.
55. Wibren van der Burg, "The Slippery Slope Argument," *Ethics* 102, no. 1 (1991): 42–65.
56. Bert-Jaap Koops, "The Concept of Function Creep," *Law, Innovation and Technology*, 1 (2021): 29–56, https://doi.org/10.1080/17579961.2021.1898299.
57. The fact that the expansion of scope was regulated does not hinder the fact that it is still an expansion of scope that was not foreseen in advance.
58. See also the principle of purpose limitation in data protection explained in Chapter 4 in this Volume.
59. Council Decision of 8 June 2004 establishing the Visa Information System (VIS), OJ L 213, 15.6.2004, p. 5–7.
60. Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), OJ L 218, 13.8.2008, p. 60–81.
61. Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications. A Comparative Legal Analysis*, *Privacy and Data Protection Issues of Biometric Applications* (Dodrecht, Heidelberg, London, New York: Springer Netherlands, 2013), https://doi.org/10.1007/978-94-007-7522-0.
62. Scholars usually refer also to virtue ethics (VE). For clarity reasons, VE approaches were not included because they are not widespread 1) in the debates on border control, and 2) in the assessment methods overviewed in Section 5.1.6. For more information on virtue ethics and technology, see Shannon Vallor, *Technology and the Virtues. A Philosophical Guide to a Future Worth Wanting* (New York: Oxford University Press, 2016).
63. Immanuel Kant, *Groundwork in the Metaphysics of Morals* (Cambridge: Cambridge University Press, 2012).
64. High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI."
65. See Chapters 3 and 4, in this Volume.
66. High-Level Expert Group on Artificial Intelligence.
67. For example, European Border and Coast Guard Agency (Frontex), *Code of Conduct Applicable to All Persons Participating in Frontex Operational Activities* (Luxembourg: Publications Office of the European Union, 2020). Council of Europe, The European Code of Police Ethics (Council of Europe Publishing 2001), https://polis.osce.org/european-code-police-ethics.
68. John Stuart Mill, *Utilitarianism* (Cambridge, MA: Cambridge University Press, 2014). Original work published in 1861.

69. Amartya Sen and Bernard Williams, eds., *Utilitarianism and Beyond* (Cambridge: Cambridge University Press, 1982).
70. Andrea Saltelli, "Ethics of Quantification or Quantification of Ethics?," *Futures* 116, no. October 2019 (2020): 102509, https://doi.org/10.1016/j.futures.2019.102509; Felt et al., *Taking European Knowledge Society Seriously*.
71. Trade-offs are also legally criticised from a proportionality perspective, in which fair mediation of values must be struck, as opposed to the application of the crude mechanics of scale (i.e. if one value goes up the other goes down). Jeremy Waldron, "Security and Liberty: The Image of Balance," *Journal of Political Philosophy* 11, no. 2 (2003): 191–210. See also Chapter 4 in this Volume.
72. Marc van Lieshout et al., "Reconciling Privacy and Security," *Innovation the European Journal of Social Science Research* 26, no. 1–2 (2013): 119–32, https://doi.org/10.1080/13511610.2013.723378.
73. John Rawls, *A Theory of Justice* (Cambridge, MA: Belknap Press of Harvard University Press, 1971).
74. They can also be seen as a subset of consequentialism or deontology.
75. Louise Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25, no. 3 (2006): 336–51, https://doi.org/10.1016/j.polgeo.2006.02.001; Irma van der Ploeg, "Biometrics and Privacy A Note on the Politics of Theorizing Technology," *Information, Communication & Society* 6, no. 1 (2003): 85–104, https://doi.org/10.1080/1369118032000068741; Aas, "'Crimmigrant' Bodies and Bona Fide Travelers: Surveillance, Citizenship and Global Governance"; Aas, "'The Body Does Not Lie': Identity, Risk and Trust in Technoculture."
76. Aas, "'Crimmigrant' Bodies and Bona Fide Travelers: Surveillance, Citizenship and Global Governance."
77. van de Poel et al., "Ethics, Technology and Engineering: An Introduction."
78. van Dijk and Casiraghi, "The 'Ethification' of Privacy and Data Protection in the European Union. The Case of Artificial Intelligence."
79. Mark Maguire and Pete Fussey, "Sensing Evil: Counterterrorism, Techno-Science, and the Cultural Reproduction of Security," *Focaal-Journal of Global and Historical Anthropology* 2016, no. 75 (2016): 31–44.
80. Sven Ove Hansson, "Fallacies of Risk," *Journal of Risk Research* 7, no. 3 (2004): 353–60, https://doi.org/10.1080/1366987042000176262.