Department of Political Sciences *Chair of Global Justice*

Intelligence Ethics in the Digital Age

SUPERVISOR
Prof. Marcello di Paola

CANDIDATE
Michele Cantarella
Student number 625662

CO-SUPERVISOR
Prof. Sebastiano Maffettone

ACADEMIC YEAR
2015/2016

Acknowledgements

I take this opportunity to thank my supervisor Marcello Di Paola for his essential and continuous support: without him, this work would not have been possible. Also, my deepest thanks go towards David Chuter for his insights and invaluable teachings, which inspired me and helped me shape this thesis.

List of acronyms and abbreviations

CIA: Central Intelligence Agency

COMINT: Communication Intelligence

DRS: Discriminate Reactive Spying

ELINT: Electronic Intelligence

GEOINT: Geospatial Intelligence

FISA: Foreign Intelligence Surveillance Act

HUMINT: Human Intelligence

IMINT: Imagery (or photo) Intelligence

IoT: Internet of Things

IPS: Indiscriminate Pre-Emptive Spying

ITC: Information and Communications Technology

JTRIG: Joint Threat Research Intelligence Group

MASINT: Measurement and Signatures Intelligence

NSA: National Security Agency

OSINT: Open Source Intelligence

PRISM: Planning Tool for Resource Integration, Synchronization, and Management

SIGINT: Signals Intelligence

STASI: Ministerium für Staatssicherheit

UAVs: Unmanned Aerial Vehicles

Introduction

Moral dilemmas are a constant in the intelligence profession. As a matter of fact, causing harm to someone else - be it a citizen, another agent or a whole national community - by violating laws or ethical principles has long been considered inevitable in espionage, especially if the national interest is considered to be at stake.

Such morality, however, is far from being universally considered acceptable, generating much public controversy over the last few years. Cases of human rights violation, torture and inhumane degrading treatment for the purposes of intelligence collection – such as the ones occurred in the Guantanamo Bay detention camp - have not gone unnoticed, and more recent cases such as the release of the Snowden Archives have fuelled even more controversy, as new technologies provide agencies with nearly unlimited power to monitor conversations and store personal data.

Can the national interest allow for ethical and legal concerns to be overridden in intelligence? The main purpose of this thesis is then to provide the reader with a coherent and solid moral framework for evaluating intelligence action morally, in the light of recent technological developments as well.

First, an introduction of the intelligence profession will be provided. Its traditional disciplines and practices will be analysed, exploring the three major functional areas of intelligence - Intelligence Collection, Analysis and Covert Action – and seeing how they could cause harm to other people.

Existing moral frameworks will be considered, and special attention will be given to the Just Intelligence theory, an adaptation of the Just War theory to intelligence. An original moral framework for evaluating intelligence action will be developed at the end of the first half of the thesis. We will reconsider the concept of national interest itself and eventually reach a framework based on consent as a moral compass for identifying legitimate targets and placing limits to intelligence action.

The second half of the thesis will be characterized, instead, by the introduction of the new technologies into the equation. Technological breakthrough have allowed for intelligence to achieve a quantitative and qualitative leap in performing its tasks. An analysis of how these technological advancements affect intelligence will be provided, along with exploring other trends - such as the decline of HUMINT, the proliferation of privacy-by-design applications and the use of automated drones and software in intelligence.

New ethical issues will arise, not only because of the fears of a transition towards a surveillance society, but also because moral agency gets dispersed amongst the units of a network and consent becomes impossible to ascertain, making the whole framework adopted for “traditional” intelligence crumble. The last part of the thesis will then take all the disruptions caused by technology into account and rebuild the framework previously constructed so to adapt it to a digital landscape in which intention and responsibility are diffused across the network instead of being concentrated into a few individuals.

Part I

Developing an ethical framework for conventional intelligence action

1. The nature of intelligence

Intelligence has always been associated with morally shady practices. Countless controversies have arisen over the last few years, from the abuses in interrogation in Guantanamo Bay to the mass surveillance programs enacted by the NSA and revealed to the public by Edward Snowden. Intelligence, as many argue, inevitably leads to nearly irresolvable moral dilemmas: too often, the intelligence officer has to choose whether or not hurting other people in order to safeguard the interests of its own citizens is the right course of action. The aim of this dissertation will precisely be providing the reader with a reasonable framework for analysing intelligence collection from an ethical perspective.

However, we cannot elaborate a reasonable ethical framework for intelligence action without first specifying what do we mean by intelligence. What is the role of intelligence? Why is it needed? It is necessary to provide a satisfactory definition of intelligence, of its role and its methods before going further with our analysis.

Trying to provide a comprehensive and general definition of intelligence has proven tricky. There is no common understanding of the intelligence discipline: as Warner (2002) argues, *we have no accepted definition of intelligence*. The vagueness of any attempted definition of the discipline probably originates from the enormous diversity in the methods employed by intelligence agencies, the varied nature of their tasks and the peculiarity of each agency itself. Using the words of Wheaton and Beerbower (2006) *the intelligence community, quite literally, does not know what it is doing*.

At a first glance, a basic, security-centred notion of intelligence may define intelligence as a process put in place to safeguard and maintain a state's national security and its protection against threats. With this notion, however, we may risk oversimplifying the issues at hand. The need for security does not exist in a vacuum but it is, instead, part of an all-encompassing obligation a state holds to his citizens. Angela Gendron (2005), for example, claims that intelligence is *one means by which a state pursues its obligation to protect the interests and rights of its citizens.*

Intelligence does not exist in order to directly protect national security, but to better equip democratic institutions in their task of safeguarding it.

Lowenthal (2015) provides us with what is probably one of the most popular definitions, describing intelligence as:

> *"The process by which specific types of information important to national security are requested, collected, analysed, and provided to policy makers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities"*

While touching many of the facets of intelligence, security remains central to Lowenthal's definition. Intelligence, however, is not all about protection against threats: excessive reliance on security concerns may lead to a distorted view of the whole discipline. There is more to information than just national security.

As a matter of fact, other definitions have privileged information over security, de-emphasizing the focus on threats and national security. Wheaton and Beerbower (2006), moving from Robert N. Clark's (2003) notion that intelligence professional's purpose should be to reduce the decision-maker's level of uncertainty to the minimum, define intelligence as *a process, focused externally and using information from all available sources, that is designed to reduce the level of uncertainty for a decision-maker*.

This definition, while correct, may sound a little bit too general, excessively blurring the lines between intelligence and the work of other government agencies and potentially underestimating the role that secrecy plays in the process. Warner (2002) places instead much more focus on secrecy, giving us this simple definition: *intelligence is secret state activity to understand or influence foreign entities*. This definition however, may prove problematic. First, intelligence targets are not necessarily foreign, and domestic intelligence has always existed. Second, there is wide disagreement whether or not intelligence should also be used as a tool for

influencing other entities: this means that agencies have the power to intervene directly into issues while, to many, intelligence should only be considered as the tool for providing information to the power. This is one of the reasons why covert action – one of the most controversial aspects of intelligence – has often been considered as separate from the intelligence process.

David Chuter (2011) then provides us with a simple yet elegant definition, incorporating concerns over secrecy and leaving the direct intervention facet aside for the moment, defining intelligence as:

> *"The process of acquiring and making use of information from an entity - not necessarily a state - which that entity does not want you to have, without them realising you have acquired it"*

As we have seen, central to many definitions of intelligence is a reference to states and legitimate authorities as the employers and beneficiaries of intelligence. While private intelligence agencies is on the rise and public-private partnerships are a not unknown of (see Michaels, J.D. 2008), it is important to remember that intelligence still remains a mostly national affair. "Traditional" intelligence agencies are, after all, government agencies. Even if the definitions adopted de-emphasize security, intelligence is still commonly considered as a tool for enabling governments to better purse their obligations.

Governments need intelligence for a variety of reasons. Many of these reasons are embedded in the definitions we have just provided: enable the state to "pursue its obligation to protect its citizens", to "reduce the level of uncertainty" or just to "make use of information". Put in other words, governments run on information, and some kind of information may not always be available through conventional means. There is a line of conduct for retrieving information, a line that many other governmental agencies do not cross: that's when intelligence comes around. Intelligence then satisfies two requirements: it gathers and processes information that is 1) relevant and 2) not available otherwise (Chuter, 2011).

The relevance criterion is fundamental: intelligence does not serve the needs of policy makers only by providing raw, unfiltered information. For what concerns analysis and collection, *all intelligence is information,* but *not all information is intelligence* (Lowenthal 2014): intelligence is information that is identified, obtained, and analysed in order to tailor the needs of policy makers.

Helping us find an answer to the question "why do governments needs intelligence?", Lowenthal (2015) comes in our aid identifying four major ways intelligence agencies provide support to the policy-maker: *to avoid strategic surprise; to provide long-term expertise; to support the policy process; and to maintain the secrecy of information, needs, and methods.* Intelligence agencies serve, then, specific functions that are considered by many to be vital for the correct functioning of a state or, better, for the state to enact its obligations towards its citizens.

One last thing before we go further. The fact that most intelligence agencies are governmental agencies has not been stressed enough. Intelligence organizations share similar motivations and a common political culture with other government agencies, as they are part of the government and they work for it. Intelligence officers are still government servants, paid by taxpayers and whose work is subject to the control of democratically elected (best case scenario) governments, which are ultimately accountable to their own citizens. There is, as Lowenthal (2014) puts it, *a semipermeable membrane* separating policy-makers and intelligence officials. As the scholar argues, this membrane is semipermeable since it allows policy makers to cross over into the intelligence sphere, inhibiting intelligence officials from crossing over into the policy sphere.

Of course, there are many other differences: intelligence officers need to be able to "fit in" and convince everyone else they are not spies (they may have to pretend to be diplomats, or work undercover); they also require developed human or analytical skills. Since they need to be able to manipulate or deceive other people, making them do what they may not want to do, intelligence officers have access to expertise that other government servants have no access to. And, of course, let us address again the elephant in the room: yes, intelligence organization engage in activities that not only

some people regard as antithetical (Lowenthal, 2014) but also that any other government agency would refrain to engage in. And these activities are covered under a veil of secrecy that, for obvious reason, no other agency deploys.

Therefore, picturing intelligence officers as much less compelling government servants may not be entirely correct, but highlighting the shared culture – along with shared practices and restraints – between the professions helps us move away from a romanticized version of the work of the "spy" we may be accustomed to.

This brief outlook at the nature of intelligence may suggest us that some limits for intelligence action may already be in place. After all, being government agencies themselves, shouldn't intelligence agencies conform to the same principles a national community – or the state, or the government – stands for? Or, at least, shouldn't intelligence agencies be subject to a degree of control from an authority that is committed to these same moral and legal principles? We will now see how these limits have been – or may be – breached.

2. Intelligence and the inevitability of the moral dilemma

Any intelligence agency will, sooner or later, face the inevitability of moral dilemmas in their job. After all *the use of secret agents - voluntary and non-voluntary - is intended to provide valuable information believed to be unobtainable* (Perry, 1995). Where conventional methods fail in the task of retrieving such information, here intelligence agencies step into the game. In other cases, this issue has led many (like Omand and Phythian, 2013) to argue that intelligence officers are constantly presented with *moral hazard* in their profession. The definition of moral hazard used by the two authors is different to the one we are usually presented with in economics: simply put, due to power and information asymmetries, intelligence officers are put in position in which actors do not share the same benefits and risks. In other words, intelligence agencies can create negative externalities for which their officers are not held accountable for due to their obligations towards the national interest.

As Omand (2013) explains, intelligence collection may require extraordinary methods that relate to a whole different set of morality principles than the ones we use in our everyday life. As a matter of fact, causing harm to someone else - be it a citizen, another agent or a whole national community - by violating laws or ethical principles has long been considered inevitable in espionage, especially if the national interest is considered to be at stake. Of course, intelligence gathering is not always unethical or illegal. But, for its nature, there are cases in which the lines are blurred, or in which the morality of an action is disputable, at best.

Both governments and intelligence communities are, of course, aware of this issue. If we go back in time up until the Congress act in 1947, which led to the creation of the Central Intelligence Agency, we will find that the Agency was authorized to pursue its tasks by undertaking "special projects". A denomination that, according to commentators like David L. Perry (1995), clearly signalled that potentially ruthless methods of intelligence action were envisioned from the inception of the agency, as later confirmed by a 1954 report from president Eisenhower (see Doolittle, 1954), who claimed that the US had to employ *more clever* and *more ruthless* methods in order to be able to *subvert, sabotage and destroy* its *implacable enemy*. The implacable enemy, of course, was the Soviet Union and, as Perry (1995) reports, the President added that justifying these methods entailed a *fundamentally repugnant philosophy*.

Of course, as much as there are many people tolerating these methods, there are many others rejecting them, some demanding more oversight on intelligence agencies, some others going as far as advocating their complete dismantling. But very few people would dispute the claim that president Eisenhower's statement is, up to a certain degree, true, and that, in order for these agencies to perform their tasks, sometimes a more "flexible" conception of morality is required. After all, rooted deep in our minds, we all expect intelligence agencies to operate at the boundaries of morality, sometimes "getting their hands dirty" when a "greater good" is at stake. There is nothing surprising about this narrative.

As we just mentioned, such morality is far from being universally considered acceptable, and many more controversies have arisen over the last few years, when, after the 9/11 attacks, intelligence gathering has started to "take his gloves off" much more than in the past (Pfaff, Tiel, 2004). While during the Cold War the actions of these agencies benefitted from a tacit approval from society and a much less criticism, now not only the methods employed by these agencies are contested from an ethical standpoint, but also the purpose and the efficacy of the intelligence profession itself are going under fire. Consequently, recent controversies have generated much more vocal criticism than in the past.

It is an issue that has also gained a degree of institutional recognition. The Parliamentary Assembly of the Council of Europe has voiced their concerns over intelligence practices and standards on multiple occasions. In 2005, in its report on the *Democratic oversight of the security sector in member states,* it called upon the drafting and adoption of a European Code of Intelligence Ethics - in the same fashion as the European Code of Police Ethics.

As stated in article 10 of the declaration, the Assembly "[…] *recommends that the Committee of Ministers prepare and adopt guidelines for governments setting out the political rules, standards and practical approaches required to apply the principle of democratic supervision of the security sector in member states, drawing on the following principles:* […[1]]".

Later, in their 2007 second report on *Secret detentions and illegal transfers of detainees involving Council of Europe member states*, the Assembly demanded

[1] For what concerns intelligence services, the Assembly asked for the following principles to be followed:

a. The functioning of these services must be based on clear and appropriate legislation supervised by the courts;

b. Each parliament should have an appropriately functioning specialised committee. Supervision of the intelligence services' "remits" and budgets is a minimum prerequisite;

c. Conditions for the use of exceptional measures by these services must be laid down by the law in precise limits of time;

d. Under no circumstances should the intelligence services be politicised as they must be able to report to policy makers in an objective, impartial and professional manner. Any restrictions imposed on the civil and political rights of security personnel must be prescribed by the law;

e. The Committee of Ministers of the Council of Europe is called upon to adopt an European Code of Intelligence Ethics (in the same fashion as the European Code of Police Ethics adopted by the Coucil of Europe);

f. The delicate balance between confidentiality and accountability can be managed to a certain extent through the principle of deferred transparency, that is to say by declassifying confidential material after a period of time prescribed by law

intelligence agencies to undergo a profound revision of their practices, and to be subjected to *codes of conduct, accompanied by robust and thorough supervision*. Also, in 2015, a similar call for better regulation on agencies was reiterated, specifically on the issue of mass surveillance. Again, the Assembly demanded Member Countries to agree on a multilateral *Intelligence Codex for their intelligence services*, laying down common rules in the cooperation for the fight against terrorism and organised crime, setting up specific limit for intelligence, advocating for a ban of the use of surveillance measures for political, economic or diplomatic purposes among participating states. All these calls for better regulation and better standards reflect a common sentiment amongst societies suggesting that, as Bellaby (2012) comments, as long as liberal democracies are supposed to abide by the rules, norms and ideals to which they subscribe, then so must their intelligence communities.

The argument for a definition of a moral code for intelligence has thus been increasing its legitimacy over the past few years, ceasing to be treated as a ridiculous oxymoron. Increased awareness on the issue is, however, insufficient for solving the inherent moral tension that accompanies intelligence action. As Bellaby (2012) argues, intelligence communities face a tension created by the *duty to protect a political community* and *the reality that intelligence collection* (and intelligence action in general) *may entail activities that negatively affect individuals*. Many have tried to solve this tension by providing different moral frameworks for intelligence: needless to say, there is hardly any agreement here.

Is it possible to justify some of the most controversial methods of intelligence just because these means served a nobler end? Or do intelligence agencies have to comply with some specific moral constraints as much as every other governmental agency? If we can have a universal system of values for certain spheres of human action like warfare and many others, why is this not possible for intelligence? And, if establishing an ethical framework is possible, how do keep intelligence agencies accountable if their work is kept secret? In this first part of the dissertation, we will attempt to provide the reader with an answer to such questions.

3. "Taking the gloves off": some practical examples

We need some practical examples first. As we cannot solely rely on James Bond movies to get a good idea of the moral dilemmas intelligence professionals often face, we will try to draw some theoretical or real life examples, exploring the three major functional areas of intelligence - Intelligence Collection, Analysis and Covert Action.

3.1- Intelligence collection and its issues

Intelligence collection is the first and probably most important area of intelligence. It is *the bedrock of intelligence* (Lowenthal, 2015): without collection, no analysis (nor adequate response) would be possible. This does not mean that some of its methods, however, have not raised controversies. Of course, many intelligence gathering methods are mostly legal and innocuous. But still, there are many more cases where the lines between what is good and what is not are blurred. For this reason, the main focus of our study will be intelligence collection.

Intelligence collection is made up of many disciplines, employing different tactics and strategies for gathering vital information. The methods employed usually depend on *the nature of the intelligence being sought and the ability to acquire it in various ways* (Lowenthal, 2014): some information can only be retrieved through specific methods. While a detailed analysis of such disciplines goes beyond the aims of this study, it is worth mentioning some of the most important ones.

HUMINT – Human Intelligence, also known as the world's second-oldest profession – is probably the most popular collection discipline. All intelligence collected through interpersonal contact is categorized as Human Intelligence. As Lowenthal (2014) reports, the majority of HUMINT involves dispatching clandestine service officers to foreign countries, where they attempt to recruit agents: spies, foreign nationals that can provide them with the information they need.

Technical collection disciplines are much more varied instead, ranging from geospatial intelligence (GEOINT, formerly imagery intelligence or IMINT), to signals intelligence (SIGINT), and measurement and signatures intelligence (MASINT), and many other sub-disciplines.

Amongst these disciplines, SIGINT is of particular interest for our purposes. SIGINT – signals intelligence – is a relatively modern discipline, pioneered during World War 1, when British intelligence managed to intercept German communications by tapping underwater cables (Lowenthal, 2014). All SIGINT refers to the collection of intelligence by the interception of signals. There is great diversity in the items intercepted by SIGINT: they can be communications between two or more parties (and here the term COMINT – communication intelligence – can be used), electric emissions from military and civilian systems (FISINT – foreign instrumentation signals intelligence, or more commonly ELINT – electronic intelligence), or even data relayed by weapons during tests (TELINT – telemetry intelligence.

Lastly, OSINT – better known as Open Source Intelligence - is, as Steele (2007) describes it, intelligence *based on information which can be obtained legally and ethically from public sources*. OSINT can be extrapolated from media, public data or from professional and academic publications. While less popular than other disciplines, OSINT has recently taken the lion's share of intelligence collection: the amount of intelligence collected through OSINT against the other methods of collection, in fact, now follows the 80/20 rule (Steele, 2007). OSINT is not only easily accessible and often cheap - or even free - to obtain, it is also, most of the times, completely legal to use.

As we said, some of these methods are mostly innocuous, like Open Source Intelligence collection. However, the legality and ethicality of each one of these disciplines cannot always be fully established: there are "grey areas" in which even seemingly inoffensive disciplines like OSINT can operate.

Some of these concerns have been treated merely as false alarms. Can we claim, for example, that it is morally justifiable to make use of information that has entered the

public domain immorally? Take the example of leaked information obtained through immoral means and then leaked into the Internet, should the officer restrain itself from collecting and using this information? From an intelligence perspective, the issue here may seems preposterous, as Pfaff (2005) argues, since once the information *is 'out there' there is nothing wrong with obtaining it*. It makes sense, for the logic of an intelligence officer, to make use of all the information available: what would be left of this profession if even this kind of information could not be used, considering that the damage was already done when the information was released on the public? However, we have to note that the issue of making use of "tainted" data is not unheard of: in bioethics, for example, many have already argued whether or not it should be morally permissible to use data from Nazi medical experiments for scientific research (see for example Steinberg, 2014) and this same dilemma could be applied to intelligence as well.

Hribal et al (2014) provide us, instead, with yet another example of potentially unethical use of Open Sources: an agency may use a fake social network profile in order to obtain information about the habits and interests of a specific person. In instances like this one, not only the morality of the data collection can be questionable but, as Hribal et al (2014) argue, the method of collection can also easily transition from semi-legal to illegal.

Moving back to HUMINT, we venture into much more controversial areas. Controversy has tended to focus on the topic of intelligence collection through interrogations, at least over the last decade. Think of other much discussed uses of torture and inhumane degrading treatment for intelligence gathering purposes. The Guantanamo case has surely made everyone aware of such issues: waterboarding and many other violating practices[2] were commonly used during interrogations, with the not-so-tacit approval of the government, as the – at the time – George W. Bush administration attempted to legitimize these activities through the 2002 *Bybee*

[2] As Bellaby (2012) reports, those other tactics included: *breaking chemical lights and pouring the phosphoric liquid on detainees; pouring cold water on naked detainees; beating with rope; sodomising a detainee with a chemical light and a broom stick; and using military working dogs to frighten and intimidate; hooding, hand cuffing with flexi-cuffs, beatings, slapping, punching, kicking; being paraded round outside the cells naked; exposure to loud noise; and prolonged exposure to intense sun over several hours; and even forcing a prisoner to masturbate in front of jeering captors*

Memos, which tried to redefine the very notion of torture as defined under the "Convention against torture and other cruel and inhuman degrading treatment or punishment"[3], restricting it only to activities could have caused *serious physical injury* (limiting it to organ failure, impairment of bodily function, or even death) *or mental harm that would prove to last months or even years* (Bellaby, 2012).

Of course, a moral dilemma immediately arises: could such actions be justified in the light of a common, higher good? Do our moral obligations towards respecting human rights not apply when interrogating a terrorist? What if the detainee really held vital information that could only be retrieved under the threat – and use - of torture? Would torture, in this case, be acceptable?

But there is much more than just torture, as standard HUMINT collection tactics usually entail manipulation, coercion and deception. An officer must be ready to bribe, blackmail and manufacture evidence in order to obtain information from his sources. As Perry (1995) reports, CIA officials admitted that agents were often recruited through bribery or blackmail. These methods are, then, *cornerstone tradecrafts of the collector, which test basic ethical roots*, as Caimona (2007) eloquently describes them. Like an art, these subtle techniques have been subject to continuous refining.

We are not done yet. Even maintaining a cover could easily lead to immoral behaviour. Think of an officer disguised as a terrorist in a terrorist cell, gathering information on their movements and long-term plans. The officer will, sooner or later, be obliged to engage in unethical, criminal behaviour, in order not to blow his cover up. As Lowenthal (2014) arguments, there are areas like terrorism and narcotics in which intelligence collection relies heavily on human contacts: contacts must be developed with criminal organizations – and money may be paid to them – so as to enable successful penetration in the organization. Would in that case

[3] Accordingly, *the term "torture" means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity. It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions* (Art. 1).

criminal actions – like murdering innocent people, trafficking drugs, participating in terrorist attacks, etc. – be justifiable in the light of a higher good?

Moving back to the realm of SIGINT, we can only think of the recent developments in information and surveillance technology, granting agencies with a nearly unlimited power to monitor conversations and store personal data. The revelations coming from the Snowden Archives have shown how the recent technological developments have led to a quantitative and qualitative breakthrough in Signals Intelligence. Leaking hundreds of classified documents detailing the mass data-gathering plans of the NSA and its American and British partners, Edward Snowden managed to shift public attention on intelligence gathering issues from interrogation practices – a debate that pretty much characterized the previous decade – towards a whole new set of ethical dilemmas.

The archives showed, amongst many other revelations, that phone companies were sharing their consumer data with the NSA; that private conversations were data mined and monitored by the NSA with the collaboration of ITC giants such as Apple, Google, Facebook and Microsoft; that the United Kingdom Government Communication Headquarters were monitoring global communications and sharing the data collected with the NSA; and that geo-localization information and financial transactions were monitored too (Berendt et al, 2015). These leaks obviously led to the growing apprehension of many commentators, worried about the uses of technology in a surveillance society, some going as far as claiming that a social contract between the state and its citizens had been breached (see Berendt et al, 2015). Was this severe violation of privacy justifiable in the light of a higher good? Was this really being done for the national interest?

3.2 Intelligence analysis and its issues

Controversy has tended to emphasize the misconducts of intelligence collection and covert action, and rightly so. This does not mean that intelligence analysis may not present its own set of ethical issues as well. To provide the reader with a

satisfactory definition, Intelligence Analysis is *the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context,* as defined by Johnston (2005).

Analysis is one of the pillars of the intelligence process, providing policy-makers with senseful and organized information extracted from a continuous stream of data. Its function is to advise and better inform the policy makers on *the issues they face and the decisions they have to make* (Lowenthal, 2014). It is, mostly, a work devoid of moral choices, but while we too will prioritize the issues inherent with the operational side of intelligence, it is worth mentioning some of the concerns that may arise with intelligence analysis.

Bad advices usually do more harm than good. As Lowenthal (2014) argues, intelligence officers have the duty to "*tell the truth to power*": the analysis should not be tainted by the always-looming risk of incorporating personal bias into it, deliberately or not. The analyst holds then a responsibility to maintain his objectivity and professional integrity. Chomeau and Rudolph (2006), in an attempt to apply principles of business ethics to intelligence analysis, specify those prescriptions, adding that analysts should refrain from *getting involved in the formulation and implementation of policy*, mindful not to *construct their analysis so as to favour one particular policy position over another*. Accordingly, the only obligation of the analyst *is to the truth*.

These are pretty straightforward moral prescriptions: as long as an analyst maintains his integrity, he should have no doubts he is not committing any moral wrong. However, analysts too can face moral dilemmas. For example: how should an analyst behave if others politicize his "product", as Chomeau and Rudolph (2006) ask? And Lowenthal (2014) presents us with even more dilemmas: What if the analysis is ignored and the analyst believes he should take a stand and not temper his analysis for the sake of his long-term relationship with policy makers? And what would be the correct line of conduct if the policy-maker pressured the analyst to produce intelligence that supported government's policies?

3.3 Covert action and its issues

Finally, we have covert action. Covert actions are, as Lowenthal (2014) defines them, *interventions by one state into the affairs of another*. This definition does not necessarily involve intelligence agencies, hinting at another overarching issue of this study: intelligence studies have been long characterized by a *perennial debate* about whether covert action should be considered as part of the 'intelligence' process or not, as Omand (2012) argued. Phythian (2013) points out that no consensus exists on whether intelligence should be understood as including covert action or not.

This confusion may stem from a number of reasons, the most compelling one being that, in some countries, both covert action and intelligence tasks are carried out by the same organisations, as Chuter (2011) claims. Also, covert action relies on the intelligence collected and analysed by intelligence agencies, this also leading to some confusion. Untangling this misunderstanding is pretty important since the answer we give to this problem depends on our whole conception of intelligence and has deep consequences on the moral framework we may want to adopt. Whether we see intelligence agencies has informers and advisors of governments or whether we see them as an operative hand of the governments too, ready to dirty its own hands: the perspective chosen will change a lot of things.

To support the thesis that covert action cannot be considered part of intelligence, we can say that a number agencies and countries refrain from carrying out covert operations. As a matter of fact, as Lowenthal (2014) argues, *many states do not have the capability, the need or the will to carry out covert actions against other states.* On the contrary, others, like the CIA instead, have been known to use covert action much more extensively.

For now, we will assume that covert action are part of the intelligence process and later evaluate whether we covert action is compatible with the same moral standards that we apply to collection and analysis. For this purpose we will include some examples of covert action and how they managed to raise controversies, and we will get back to the point later. There are plenty of examples – mostly involving the CIA

and US government – of covert actions carried out to interfere into the affairs of another state.

Take the example of US intervention in Nicaragua in the 1980s. This is pretty useful example, since here US and CIA intervention became *as overt as covert policy can be* (Forsythe, 1992). The Reagan government authorized and organized covert military attacks against the Sandinistas as early as 1981, dragging the country in a civil war that would have led to the death of more than 30,000 Nicaraguans. The CIA was directly involved, training, funding and organizing *contra* forces, and advocating the neutralization of civilian officials and condoning military attacks on civilians in its training manuals (Forsythe, 1992). Of course, human rights protection under the Sandinistas was inconsistent and imperfect, but, under international pressure, the government started scaling up its commitment towards human rights (especially socio-economic ones) and even held presidential and legislative elections in 1984. These efforts did not stop covert action in Nicaragua: as Forsythe (1992) reports, human rights were never a concern for the US and the CIA, as the Reagan administration had decided that the presence of a Nicaraguan government with ties to the USSR was a threat by itself.

Can we consider this kind of intromission in another state's affairs acceptable, especially when the civil war that ensued claimed so many lives? In whose interest were these actions carried out: the Nicaraguan people or the US government? Take also the example of US intervention in Chile in 1973. Here, intervention differed because 1) Allende's government was democratically elected and fully committed to human rights and 2) intervention was much less direct and took the form of indirect of the anti-Allende coalition. Again, what justifies these actions, from a moral standpoint? And can forms of indirect intervention be considered more acceptable, instead?

Let us put everything in order. With covert action, the main issue is one of legitimacy. It is clear that, in the eyes of the agency, the legitimacy of such actions only rest in the legitimacy of the authority issuing the order. But what may look a legitimate concern for the American government – as in the example illustrated above – may not be as legitimate in the eyes of the Nicaraguan government or

people. A ruthless, realist approach to international relations may see these actions as perfectly legitimate, for the state ordering them. But this approach would be unacceptable for our aims without tumbling into the pitfalls of moral relativism, as we develop a comprehensive, universal, general approach to intelligence ethics.

Let us get the national interest of that one state issuing the order out of the question. What if, instead, those covert actions are really in the interests of the citizens of the targeted state – an option that is, at best, fairly unrealistic? As Lowenthal (2014) asks, *are such operations legitimate against oppressive, undemocratic regimes but illegitimate against those with more acceptable forms of government*? The problem is still the same: who gets to decide whether those governments are legitimate targets or not?

This is just a short list of examples of moral dilemmas. We will see, later, if some of these cases may not be considered ethically admissible, even if the national interest is at stake, and when some other may be. Is it possible to build an ethical and legal framework for intelligence that is perfectly compatible with the national interest?

This is precisely the problem: a great deal of intelligence work is morally questionable: is it possible to justify some of it? Or is the whole profession ethically objectionable because it relies on wrong premises?

4. Common approaches to intelligence

As with any other human activity, many have tried to adapt intelligence into existing moral frameworks, with varying degrees of success. Literature seems to focus on a limited number of popular approaches: the nihilist, the realist, the utilitarian and the idealist. Just war theory has also been applied to intelligence, but this is a point that will be elaborated further in the next paragraph.

Starting off with our first approach, it would be easy to assume that intelligence officers need to adopt a nihilist approach in their profession. And it is not uncommon

for them to be portrayed as such by popular culture. After all, **moral nihilism** provides intelligence officers with an excellent excuse for disregarding moral issues that could arise over the course of their job. This approach allows officers to ignore the harm being made to people, as there is no intrinsic reason why they should regards the rights and the dignity of other people, if we believe moral claims to be social constructions and nothing to be inherently good or wrong. It is difficult, however, to make this position look convincing: moral nihilism is not a moral theory by itself; it is a rejection of ethics itself, as all moral claims are meaningless, and no moral belief is justified. These problems render moral nihilist pretty much incompatible with the intelligence profession, leading Pfaff (2006) to lists moral nihilism as the first misunderstanding of the ethics of the intelligence.

Not to be confused with the nihilist position, we have **political realism**. This approach, borrowed from international relations theory, is probably one of the most popular, and it *has been has been quite influential in the intelligence community for a long time* (Pfaff, 2006). It is, after all, the approach behind the aforementioned "repugnant philosophy" of intelligence. This approach starts from the core assumption that states are the main – and rational – actors in a fundamentally anarchical international system, and that, since all states have military capabilities and none can be certain of the actions of the other, their many duty is to ensure their own survival. It shares something with moral nihilism, surely, but its main claims are different: instead of claiming that ethics do not exist, it simply argues instead that *ethics have no place in international affairs*. The realist position holds a normative background: as a matter of fact, Pfaff argues that Hans Morgenthau's claim that the statesman's highest duty is to ensure national survival is applied, by extension, to intelligence professionals supporting the statesman's work.

This is the moral cornerstone of this approach: under this approach, national security issues take priority over anything else. The *Raison d'État* is too important to be tampered with moral issues. Survival supersedes any obligation there might be between nations, but also towards human right in general. Under this perspective, the well being of other citizens is irrelevant, because the only welfare gains that matter are the one of their national community. Of course, human rights and international treaties may still be respected under this approach. But this does not

change the basis for moral judgment: human rights, in the international arena, are not worthy of being respected *per se*, but only because their respect may be instrumental in pursuing higher welfare gains for the national community.

There are few doubts, however, that this approach would hardly solve our conundrum, since it does not solve any of the moral issues we encountered, but simply provided us with a theory that lacks any criteria of universality, merely describing an – already disputed – conception of international relations gravitating around the survival of the fittest. Taking, for example, the cases previously listed, this approach would pretty much justify any action in intelligence. Not only torture and inhumane practices against suspected terrorists would be perfectly justified, but any other kind of harmful action directed towards foreign citizens, innocent or not: deception, eavesdropping, theft, blackmailing and even murder could find defence under this framework.

Accordingly, the only restraints would come from matters of effectiveness: intelligence ethics scholars that have adopted this criterion as a reason for ruling off unethical behaviour (see Gendron, 2005, or Lowenthal, 2009) claim that it is unadvised to harm foreign citizens or mistreat foreign agents due to the risk of international repercussions or due to these methods losing their efficacy in the long term.

Realism therefore surely makes sense as approach for international relation, but this does not make it less morally undesirable, as it will always fundamentally based on inequality and injustice: the only moral compass for intelligence essentially rests in the hands of hegemonic powers. It is not surprising, for example, that a realist discourse was adopted to justify the aforementioned US and CIA intervention in Nicaragua. And, even if realism leads to intelligence officers behaving more ethically for the sake of effectiveness, it is still questionable whether respect of human rights and dignity should be a mean to achieve an end and not the end itself. This raises the question whether the national interest could be treated as *a sufficient guide to the ethics and morality of intelligence*, as Lowenthal (2008) wonders.

Discussion about means and ends lead us to the next approach. Against realism, on the opposite side of the moral spectrum, we have the **idealist approach,** which stresses the concept of moral duty (as Gendron, 2005 describes it), drawing heavily from Kant's moral philosophy. As Kant's categorical imperative imposes us to treat people as ends not as means, this approach pretty much rules out most of the actions intelligences might be engaged in. Torture, deception, manipulation, eavesdropping and many more activities are simply not allowed, as they all entail breaking this prescription, leading to an unconditional condemnation of pretty much all espionage activities.

Also, borrowing from Kant's Perpetual Peace, morality should also preclude democratic states from engaging in espionage activities, since, as Gendron (2005) explains, *stealing other peoples' secrets by listening to or reading their private communications is improper because the assumption is that various individuals and societies are part of a "civilized" community sharing basic values*. More specifically, item 5 and 6[4] of the preliminary articles for perpetual peace among states contain principles that essentially rule out intelligence activities. There are few doubts that covert action is prohibited under these articles, as it consists in an act of interference with the constitution and government of another state (art.5), an unambiguous act of hostility, which would make mutual confidence in the subsequent peace impossible (art.6). Also, art.6 explicitly rules out interventions like "employment of assassins (*percussores*), poisoners (*venefici*), breach of capitulation, and incitement to treason (*perduellio*) in the opposing state" listing them as acts of hostility.

There is no need to explain that some of these interventions are clearly undertaken over the course of covert action activities. There is, however, more than just covert action, as intelligence activities in general are explicitly excluded too: if we look again at article 6, not only it is clear that many intelligence collection activities may classify as acts which would make mutual confidence impossible (and there is plenty of

[4] (5) "No State Shall by Force Interfere with the Constitution or Government of Another State"
(6) "No State Shall, during War, Permit Such Acts of Hostility Which Would Make Mutual Confidence in the Subsequent Peace Impossible: Such Are the Employment of Assassins (*percussores*), Poisoners (*venefici*), Breach of Capitulation, and Incitement to Treason (*perduellio*) in the Opposing State"

literature and real life examples[5] on how spying one's neighbour leads to deterioration of mutual trust and increases in international tension) but here Kant explicitly addresses espionage as an *intrinsically despicable* activity, an activity which exploits the *dishonourableness of others* even in times of peace.

Surely, attempts, such as Pfaff & Tiel (2006), have been made to adapt intelligence operations under the Kantian approach, but these attempts have inevitably swayed away from Kantian idealism. While the moral theory they end up developing is surely one of the most interesting approaches to intelligence ethics and a fundamental source of inspiration for this study (as we will see later), it cannot be helped to notice that, when controversial methods of intelligence[6] end up being permitted, we cannot talk of Kantian idealism anymore. Sure, circumstances may necessitate contravening to moral laws, but Kant's view is clear: spying is "intrinsically despicable". Kantian idealism entails a total rejection of intelligence practices, as the national interest itself coincides with fully respecting these categorical imperatives. But what's left of the intelligence profession when idealism rules out most of its activities?

Finally, we have the **consequentialist approach** (and the similar pragmatic approach), sitting at the middle of the spectrum. Moving from Bentham's classical utilitarian theory, this approach takes the axiom "it is the greatest happiness of the greatest number that is the measure of right and wrong", applying it to intelligence. What makes an obligation "higher" than another one? There is no national interest or any inviolable moral commandment here: this approach simply assumes that welfare is quantifiable, and – put simply - the action that maximises this welfare is the only good one. It comes without saying that this welfare is absolute, and not simply relative to a national community: otherwise, we would just be dealing with a variation of the realist approach.

[5] See Pfaff (2006) to see how the Jonathan Pollard case strained the relationship between US and Israel. German Chancellor Angela Merkel's declarations on the aftermath of the Snowden revelations (hinting at massive surveillance on German communications, including Merkel's phone) are also exemplary, as she commented: "if the allegations are true, it would be for me a clear contradiction as to what I consider to be trusting cooperation between agencies and partners"; see the full article here: http://www.reuters.com/article/us-germany-usa-spying-idUSKBN0FC06P20140707

[6] We will further investigate Pfaff and Tiel's approach later; it will suffice to say, for now, that in their paper "The Ethics of Espionage" they end up condoning, under very specific circumstances, acts such as deceit, incitement, bribery, blackmail, and appropriation, while also accepting the doctrine of double effect when innocents are involved.

If torture, for example, is needed for obtaining information that could save the lives of other people, this approach could provide the perfect justification for using those methods, as the pain inflicted to the individual interrogated does not offset the loss of those lives. Kantian idealism, instead, would never allow this individual to be tortured, no matter if he is a terrorist or not. The other side of the coin is that the problem with consequentialism is that, using the same example, it would allow torture – and many other violations of human rights – no matter if that person is a terrorist or not. This approach makes no effort to identify legitimate targets or not. A perfectly innocent person may be subjected to any degree of violation of human rights, if this is the only way to obtain vital information from him.

Some final remarks: Angela Gendron (2005) also identifies a pragmatic approach, which allows that exceptions to moral rules are valid in order to fulfil a higher obligation. It starts from different premises than the utilitarian one, but the results are similar. This approach similarly argues that *the human costs of intelligence collection, in terms of the invasion of privacy or injustices against others, must not outweigh the anticipated beneficial outcome* (Gendron, 2005). However, this approach does not claim that aggregate welfare is the measure of right and wrong, it instead claims that moral obligations exist, but can be suspended when circumstances require doing so: when, for example, it is necessary to choose between two good outcomes or two bad outcomes. In this regard, this approach places itself a little bit closer to idealism.

5. Just Intelligence approaches

5.1 An introduction to Just Intelligence

Probably the most common – and apparently successful – approach to intelligence ethics is the attempt to adapt the Just War framework to intelligence. This approach has then become known as Just Intelligence, and it is a mix of realist, consequentialist and idealist approaches. Many scholars have followed this path, and

their conclusions do not divert much from one another. We will mention a number of approaches, ranging from Sir. David Omand, to Ross Bellaby, and to Chomeau J. B. and Rudolf A. C.

First of all, these approaches equate the act of intelligence gathering and analysis to the use of force in war. These approaches thus operate under the assumption that *the intelligence profession possesses power in the form of secret information, and this represents a kind of force that can be used to protect a nation's interests* (Chomeau J. B. and Rudolf A. C, 2006). Under this assumption, with war and intelligence becoming two facets of the use of force, Just War principles could be adopted for developing an ethical framework for intelligence.

Also, the notions of national community and national interests are central to these approaches. According to Chomeau J. B. and Rudolf A. C (2006), the source of the ethical dilemma for intelligence agencies lies in a degree of uncertainty over the notion of who their "client" is. We have already seen that, being those agencies part of the government, the client of an intelligence agency is the national community they are sworn to protect. The two authors agree with this seemingly unequivocal notion, and they go even further by claiming that the intelligence officer has a duty to employ the skills they are obliged to perfect solely for the benefit of their society.

Is that so? Does this statement imply that intelligence agencies not only have an obligation to protect their own community, but also to go as far as having the duty to pursue the national interest of a country? While just intelligence theory draws from many of the aforementioned approaches, these reflections reflect the risk of a realist underpinning hiding behind some approaches to the theory, and we will get to discuss this later. For now, it will suffice to say that the main duty of intelligence agencies, according to just intelligence, is to *safeguard and maintain a state's national security and, in particular, its protection against threats* (Bellaby, 2012).

The rationale behind this approach lies in a specific conception of intelligence and national security that enables the ethics scholar to find much more things in common between intelligence and military action. What is important for the adaptation of the Just War principles for scholars such as Chomeau and Rudolf is that, by identifying

the national community as the sole source of legitimacy and client of intelligence agencies, agencies are accountable for their action solely by the citizens of their national community.

Starting from these premises, Sir Omand (2013) argues that states, when considering whether or not use the force, deal with a trilemma of balancing three different propositions. These propositions come from a traditional conception of social contract, as monopoly of force is given to the state as a result of a "contract" with citizens. Accordingly, states have 1) a positive duty *to defend and protect their citizens when need arises and uphold justice and the rule of law in the face of violent challenge but (2) protecting the innocent and defending moral values sometimes requires a willingness to use force in response; and yet (3) causing harm to individuals is generally accepted as ethically wrong, including the ultimate step of taking life*. These obligations, Sir Omand argues, can as well be applied to the intelligence community.

States, therefore, according to traditional Just War theory, can fulfil these obligations by following these Just War principles:

Jus ad bellum criteria are the ones that ought to be followed in order to determine whether engaging in a war is permissible or not. Moving to intelligence, Just Intelligence advocates have adapted these principles to determine whether or not intelligence should be used, creating a set of *Jus ad Intelligentiam* criteria. *Jus in bello* criteria define, instead, the appropriate conduct in war, after its start. It relates to the legitimacy of methods and targets. Moving to the intelligence realm, the lines between *Jus in Intelligentiam* and *Jus ad Intelligentiam* are blurred: intelligence is often a continuous process, and many authors make few distinctions between the two dimensions.

1) The first *Jus ad bellum* principle, *just cause*, argues that there must be a legit reason or injury for initiating a war. As first formulated by Thomas Aquinas, these principle states that *"those who are attacked must be attacked because they deserve it on account of some fault"*. The state waging war should have been victim to some kind of injustice or aggression to justify its intervention. Of course, there has always

been a wide disagreement amongst theorists and politician on what qualifies as an aggression and what does not.

In the Just Intelligence framework this principle needs some adaptation. Intelligence collection in particular would be useless if governments could make use of it only after an aggression or injury. The same could be argued for covert action as well. Intelligence is supposed to prevent such aggressions or injuries, and therefore Ross Bellaby (2012) specifies that this just cause principle consists precisely in self-defence against threats, either foreign or domestic in nature. Thus the possibility of an attack, aggression, injury, etc. is sufficient to activate the just cause principle for intelligence. But there is more: intelligence is a continuous process, and activating it only when circumstances require it would just render it useless. Therefore, Sir Omand (2013) argues that this first *jus ad intelligentiam* condition should justify the whole maintenance and development of the intelligence machine. The just cause principle can still fully justify intelligence operations: after all, threats can lure in every corner. According to Sir Omand, as intelligence techniques are powerful but morally hazardous, it is paramount that intelligence agencies do not overstep the boundaries of just cause using their powers for illegitimate ends. This means that *the [just cause] principle is a prudent check on any tendency for the secret world to expand into areas unjustified by the scale of potential harm to national interests […] and to avoid pressure to use the intelligence machine for political or personal purposes* (Omand, 2013). Just cause principle becomes, then, a procedural condition: intelligence is legitimate only as long as it keeps working within its predetermined boundaries[7], serving its specific purposes.

2) The second principle, *just intent*, requires just cause not to be invoked for achieving other objectionable ends. In other words, as the *intention behind an act alters the moral quality of the act* (Bellaby, 2012), wrongful motives should not drive the decision to enter a war (or be pursued once the war has begun) other than the ones fitting the just cause criteria. Issues arise when we question whether the pursuit

[7] And Sir Omand identifies three proper uses of the national intelligence machine, as legally specified: national security, prevention and detection of serious crimes, and protection of the economic well being of the nation. The last one is objectionable, as not only no definition of intelligence includes it, but as it is akso debatable whether or not intelligence should also pursue economic prosperity.

of the national interest should be considered a just intention or not, even when it entails the suffering of others.

Applying this concept to intelligence, it is clear that this principle require intelligence to be used for the stated purpose and not for other objectionable political, economic, or social objectives, as Bellaby (2012) argues. Sir Omand (2013) adds that the just intent principle, when applied to intelligence, refers to a much wider requirement of professional integrity, investing every part of the intelligence process, from collection to analysis. The just cause therefore should not be used as a *pretext for a host of unrelated actions*. This principle, Bellaby adds, should also be applied to the methods employed. Using the example of property searches, he argues that officers should limit themselves to search places in which the specific offending articles may be contained. And these restrictions could be extended to the rest of intelligence: following this logic, certain methods used during interrogations, for example, should only be used if there is a reasonable chance of obtaining the information from the interrogated, and not for the sake of punishing or torturing him.

3) The third criterion, *probability of success*, entails war not to be waged if the chances of success are slim. This is a pretty straightforward principle, but some issues may arise nonetheless: what if even the smallest chance of success outweighs the costs and risks? Should war be pursued as well? Also, as it is impossible to predict the future, the authority waging war should do so making use of the information it has at its disposal. This raises issues on the quality of the information provided and the integrity of the people providing it, creating specific moral obligations for intelligence collectors and analysts, overlapping with the just intent criterion, as we have just seen.

This principle entails similar obligations within the realm of intelligence. Risk of collateral damage, to agents, to civilians, to future operations and to institutional reputation, Omand (2013) argues, should be carefully considered before approving an operation. Recklessness is, then, ethically unacceptable.

4) The fourth requirement is that of *proportionality*, and it is both a *Jus ad bellum* and *Jus in bellum* principle: accordingly, *violence of war should be proportionate to the threat that it is meant to overcome* (Bellaby, 2012). In a simple example, a nuclear attack is not a proportional response to overstepping a no-fly zone. In its more consequentialist version, this principle entails the aggregate human costs of war to be outweighed by its potential benefits.

For intelligence to be just, *the level of harm that one perceives to be caused, or prevented, by the collection* – and analysis and covert action – *should be outweighed by the perceived gains* (Bellaby, 2012). This principle goes hand in hand with the aforementioned probability of success: the potential harm caused to others should be carefully considered and minimized as much possible. This balancing between aggregate harms and gains should be made both when deciding to begin an operation (*jus ad intelligentiam*) but also when deciding what methods to employ (*jus in intelligentiam*).

Omand (2007) adds that, in order to respect this principle, intelligence operations should always adhere to an approach of *minimum necessary intrusion* – as coined by R. V. Jones – as a best practices method. It is also imperative, according to Ross Bellaby, that the gains are "just": accordingly, any gain obtained from the operation should comply with the principles of just cause and intent, otherwise it should be considered null or morally unacceptable.

5) The fifth criterion is the one of *last resort*. According to this rule, *when just cause could be achieved by non-violence means, then the party has a moral duty to prefer these methods* (Miller, 1991). War should be waged only if it is the only way to achieve the just cause, and other less harmful paths (such as diplomatic or economic pressure) have been explored.

This concept is a little bit different for intelligence, due to its different nature. Here the last resort principle does not prevent intelligence collection or analysis from happening, but rather certain methods to be employed: as long nonviolent and nonintrusive means can be employed, there is no morally compelling reason for treating intelligence as a last resort option. Looking at intelligence gathering, for

example, the officer should first look into open sources and other non-harmful means, and if the information cannot be reasonably obtained through these methods, then other secret intelligence methods can be employed, as Omand (2013) argues. Due to these adaptations, we can claim that the last resort principle resembles the proportionality principle much more than in its just war counterpart and, as such, many authors (such as Chomeau and Rudolph) have treated the two principles together.

6) The last principle of *jus ad bello* is the one of *competent authority*. War should only be waged by a legitimate authority, which can be held accountable to its people. Just authority should act as the last safeguard after all other criteria have been met. Central to this concept is the notion of sovereignty: here states are bestowed with a moral authority that non-state actors lack. This of course raises some interrogatives: what if the government is not democratically elected, does it still have the right to wage a war? The authority and the exclusive moral standing then reside and intrinsically depend on the legitimacy of the state: there are few doubts that solid democratic institutions are able to guarantee this legitimacy.

In a similar fashion, just intelligence requires a legitimate authority that could both mandate and oversee the intelligence process. As Bellaby (2012) argues, this authority is here to represent the wishes of the society and grant legitimacy to the intelligence process. But here we have a first problem: how is it possible to hold this authority and intelligence agencies accountable while maintaining the secrecy of the intelligence process? Sir David Omand (2007) comes in our aid, maintaining that, for this criterion to be respected, intelligence needs a *proper oversight from outside the intelligence community and a robust mechanism where any individual issue raised can be done so without fear, yet done in ways that will protect the essential secrecy of the business*. He argues that for intelligence to be just, authorities and agencies should comply with strict principles of procedural justice, while still holding the government – and the appropriate ministry – ultimately accountable for the actions of the agency.

7) The other *jus in bello* principle is the one of *discrimination*. No war has ever been made without shedding blood. Killing may be necessary on the battlefield, and

just war advocates argue that a war can still be a just one even if it requires the killing of other people, as long as these targets are legitimate. According to Michael Walzer's (2006) argument for Discrimination and Combatant Equality, all combatants, by willingly engaging in a fight, lose their *title to life and liberty*. The act of fighting then allows for the principle of discrimination to take place: while killing non-combatants is forbidden because they still regain their right to live, the killing of other combatants is allowed precisely because their right has been revoked. This principle then argues that military attacks *must discriminate between combatants and non-combatants* (Bellaby, 2012). Of course, this argument has not been received without criticism: the line between combatants and non-combatants have blurred in modern conflicts, while the collateral death of civilians may still be permitted under the double-effect exception. These problems also transfer to just intelligence approaches.

Just intelligence proponents argue that this principle requires discrimination between targets, especially in intelligence collection. As Bellaby (2012) puts it, *just as soldiers waive their protective rights by acting in a threatening way, so too can any individual act in such a way as to make himself threatening and forfeit his protective rights*. Pfaff and Tiel (2006) too, while not arguing in favour of a just intelligence approach, argue that the key discriminant between targets is the *consent* the individual gives to *participate in the world of national security*[8]. Bellaby (2012) specifies that any individual that has made himself a part of the threat can be considered a legitimate target.

5.2 Limits of Just Intelligence approaches

This was just a general introduction on Just Intelligence frameworks. Naturally, approaches vary slightly, with some authors privileging certain aspects of the tradition and others, instead, excluding other elements. But, still, we argue that it is possible to identify some common central elements that bring these frameworks together. And, precisely, criticism on Just Intelligence approaches focuses on these elements.

[8] The two authors propose a detailed framework for distinguishing the level of consent given by the target. But we will get to this point later, considering that their approach cannot be considered part of the Just Intelligence theory.

The problem with Just Intelligence approaches is that respecting their criteria does not necessarily make intelligence more just. As Phythian (2013) claims, actions that are blatantly in violations of human rights and international conventions – and that can be clearly morally questionable acts – may be perfectly permissible under a just intelligence framework. It is interesting that these actions may be so reprehensible that governments may still need to hide or disguise them so to avoid public backlash, even if, under just intelligence approaches, these actions would be perfectly sound and justifiable. Let us take back the example of Nicaragua, for covert action: here there was a clear violation of the just intent principle. The US, in fact, declared that its action were done with the purpose of re-establishing democracy, but the real reason why the CIA conducted covert action in Nicaragua was because of the threat of a Soviet affiliated state in a region traditionally under the United States' influence sphere. It is interesting that the real reasons behind the intervention may fit perfectly as a just cause prerequisite (given that a just authority identified the regime as a threat to US security), yet the US government preferred to hide its actions.

The same holds true for intelligence collection. What happened in Guantanamo Bay may look perfectly justifiable under Just Intelligence frameworks, and so could NSA's work (as the violation of citizens' privacy may be considered as collateral damage under the double-effect doctrine). Yet US government felt the need to redefine the crime of torture and refrained from revealing NSA acts to the general public (and when information leaked criticism was almost universal). This suggests us that there may be something inherently wrong with Just Intelligence theories.

First, in war, targets are either "black or white": they are either combatants or civilians. This is different in intelligence, where there is no real demarcation between actors involved in national security and ordinary people: there are, rather, various degrees of participation in the intelligence game. Distinguishing between legitimate and illegitimate targets without taking in consideration that different roles in the intelligence game may correspond to different expectations and different moralities is without doubt one of the greatest limits of just intelligence, as this principle exposes innocent people or even individuals who are only partially involved in national security issues to harm.

There is no justice to be found when innocent people are hurt by the actions of intelligence agencies, no matter if the probability of success were favourable of if the criteria of proportionality were respected. This is not a framework that can justify everyday violation of deeply embedded moral norms. Wars are, as Phythian (2013) argues, an exceptional event. In exceptional circumstances, certain moral norms may exceptionally be suspended, hence the need for Just War frameworks. Intelligence is, instead, a continuous process. It needs coherent and universal moral standards that can be considered acceptable in every moment, as *the distinction between "peace" and "war" has no intelligence equivalent* (Phythian, 2013).

Moreover, another criticism stems from the fact that just intelligence frameworks deprive the intelligence officer from his moral agency, placing it outside of his control. Just intelligence frameworks believe that moral decisions can be taken at a level higher than the individual, equating the role of the officer to the one of a soldier. This picture, however, strides with reality: as Reed (2016) argues, officers benefit from a much wider degree of discretion in their work, and many of the moral dilemmas encountered in intelligence are faced at an individual level, making the officer directly responsible for his actions. The reality is that officers and authorities cannot wash their hands from any controversy simply by justifying it in the name of the national interest, even if just intelligence principles are respected.

The reason behind these issues is, as Phythian (2013) argues, that these approaches *involve subjective judgments taken in specific national contexts*. Who decides if the "cause" is "just" or not? It is just authority, we may answer, which acting in the national interest – the ultimate source of legitimacy in these frameworks – identifies whether a cause can be considered just or not. But here we may argue that different national interest can collide, and that what is just and acceptable for a given state may be completely intolerable and wicked for another one. This does not mean that intelligence should not take orders from national governments, but rather than these orders do not necessarily make intelligence action morally sound. "Just cause" requirements end up being artificial, empty constructs that merely reflect certain normative needs of the national interest. And

the same can be said for just authority, as it merely acts for the benefit of the national interest. None of this makes intelligence more just.

The issue is intrinsically linked to the conception of intelligence behind such approaches. We have seen that most of these approaches give intelligence agencies a specific role, which is essentially based on a misunderstanding of the role of the state on both domestic and international level. As Phytian (2013) argues, these frameworks over rely on a *Weberian conception of the state as being defined by its claim to the monopoly of legitimate violence with the idea of the "protecting state"*. While far from a "pure" realist approach, it is undeniable that just intelligence shares the same premises with realist perspectives.

After all, Sir Omand (2007) - as we have seen, one of the most influential proponents of Just Intelligence - is the first to argue that an ethically defensible position for intelligence is based on, amongst a number of other premises, this preposition: *the security and intelligence authorities are charged with the protection of the public. They have a duty to seek and use secret information to help manage threats to national security*. And if we look back on the premises of the realist theory, it is evident that both Just Intelligence frameworks and realist approaches see the states as the main rational actors in international politics, identifying survival as the main role of the state. It is obvious that Just Intelligence frameworks confer exaggerate moral normativity to national states, identifying them as the sole repository of the national interest, just as the realist theory.

It is debatable whether or not intelligence agencies may be directly charged with this duty of *protecting the public*. The lack of a widely accepted definition of intelligence inhibits us from defining what the duties of this profession are. But, as we have seen, it is difficult to believe that intelligence agencies should do anything in their power to ensure national security, considering that national security should concern them only indirectly. As a matter of fact, many scholars feel that intelligence agencies should only provide governors with information that may not be available through conventional means, and that they should restrain themselves to telling truth to the power.

Agencies are there to facilitate the role of the state to pursue the national interest, but they are not directly tasked with that duty. Here we see an obvious disconnect between realist conceptions of intelligence, holding the national interest as paramount, and cosmopolitan views prioritizing human rights. There is no right or wrong: it is obvious that intelligence agencies should work in harmony with the national interest, while adequately respecting human rights. The challenge, here, will be to accommodate both views.

If we want to steer away from realist conception of intelligence ethics, however, it is probably best to explore the possibility of circumscribing intelligence action within certain limits. To do so, however, we need to abandon some concepts and provide a redefinition of others: first of all, we need to define precisely what harm could be made to people by agencies, and in what measure it can be considered acceptable. Second, it is evident that the conception of national interest that has been adopted until now is restraining our analysis, and is in desperate need of a redefinition. Only in this way we will be able to achieve a universal framework for intelligence ethics that it is based contemporarily on individual agency, freedom and equality. This does not necessarily imply abandoning the whole just intelligence framework, but rather accepting its general limits while redefining and adapting it to our necessities by focusing on some specific elements.

Also, it is probably time to place a distinction between covert action and intelligence collection/analysis. So far, we have treated them together, as the operational history of influential and important agencies such as CIA encompasses all the activities equivalently. However, our latest considerations make clear that covert action and gathering cannot answer to the same moral framework anymore. Treating them together under the analytic umbrella of intelligence ethics has only muddied our waters, and it is probably one of the reasons behind this confusion. Covert action may perfectly fit the criteria for exceptionality that makes war legitimate under Just War framework. We can argue that a Just War approach is perfectly adaptable to covert action, as it shares significant similarities with war. The same cannot be said for intelligence gathering, as it is an everyday activity that takes place even during peacetime.

6. Are there any limits of intelligence?

6.1 Legal limits

Before going further, we must assume that there must be some limits to intelligence action. It would be unwise for agencies to conduct their everyday activities unrestrained, so it is obvious that some practical limits to their action must exist. In practice, these limits are mostly legal. It is important to remember, once again, that intelligence agencies are part of the government. As such, they are bound to operate under the rule of law.

Whose law, however? There are few doubts that domestic laws have to be respected, but it is also clear that foreign intelligence works by breaking the law of a foreign country. There are still, however, other norms other than domestic laws. International laws may be an example, but there is also a body of fundamental human rights that is supposed to be respected by every country. Just to make an example, there are binding conventions, such as the 1984 UN Convention against Torture, which has been signed and ratified by nearly every country in the world: if an officer tortures another man abroad, he is still committing a crime under his own legislation.

Can exceptions to the law exist? As Giorgio Agamben (2003) argued, every constitution envisions clauses for a *state of exception*. What Agamben argues it that every political systems embeds in its constitution some kind of self-destruct mechanism that enables the same rights expressed in the constitution to be suspended or diminished, in the event of supposed national crisis. This means that, in case of emergencies, legal limits to intelligence are usually circumvented easily. The national interest apparently still takes priority over laws.

However, this mechanism is regarded as intrinsically dangerous. As Agamben argues, a prolonged state of exception leads to nothing short of a totalitarian system, an oxymoronic “permanent state of exception”. While intelligence agencies have been

know break the law or infringe constitutional rights for the sake of the national interest, it would be insane to assume that intelligence agencies can invoke this clause as much as they want. As we already argued, intelligence is a continuous process: therefore, it cannot operate in a continuous state of exception from the law. Exceptions can take place, but they have to be exceptions, literally. Intelligence needs clear and well-defined boundaries that are always valid. And, still, the existence of exceptions does not make the acts of agencies made under a "state of exception" less morally questionable.

These considerations on legal boundaries, however, do not help us solve our problems. What we need is an ethical framework for intelligence action. While morals and laws may overlap, it is important not to confuse legality with morality. Ethics are supposed to be universal, but the contingency of legality, instead, is undisputed. While dependent on morality, laws are certain and apply to everyone inside a legal community. What is legal here can be illegal elsewhere. To blur the lines between what is legal and what is ethical would be an unforgivable mistake.

Also, if a practice used for intelligence is unethical, making it legal does not eliminate the moral concern. As Omand (2013) argues, this is a common mistake that many policy-makers have made in the past, and the actions of George W. Bush, who pushed for a redefinition of the crime of torture, believing that legalizing unethical practices like waterboarding would have made such practices legitimate, act as a constant reminder of that.

Laws can also be circumvented though legal loopholes. As we will see in the second part of this dissertation, unclear legislation on wiretapping enabled the NSA to pursue much more extensive and invasive surveillance measure than before. No laws were breached, as the actions of the agency were still done within the limits of the FISA (foreign intelligence surveillance act), but the apparent legality of these methods did not make them look any less unethical to the general public when Edward Snowden released his leaks. Also, as we have already explained, exceptions can still exist: laws and fundamental rights can still be *exceptionally* breached, but these acts may still appear unethical.

These considerations suggest us that we need to move away from identifying legal boundaries of intelligence action and start on reflecting on their moral boundaries. Surely, laws can – and often do – mirror ethical principles, but the opposite is rarely true. Also, Feinberg's (1987) thoughts on the limits of legal coercion, claiming that only harm and offence to others can legitimately create grounds for legal coercion, suggest us that laws themselves may be subjected to limits embedded in ethical principles, and that we have to construct our moral limits starting from harm and offence to others. Indeed, the question whether or not legal norms pose limit to intelligence action may be preposterous, as the real problem is probably how much do laws allow intelligence to override ethical boundaries, as the Guantanamo and FISA affairs show us.

We then need to move the discussion towards the ethical limits of intelligence in order to proceed further. To define these limits, however, we need to ask ourselves first what harm could agencies do to individuals. In this way, we will be able to identify what agencies should refrain from doing on the basis on the way their actions harm other people.

6.2 Moral limits

If we want to identify what the moral limits of intelligence may be, asking ourselves what harm could be made to individuals because of abuses done by intelligence agencies is surely a decent starting point. This will help us define a bit better the moral boundaries of intelligence. Here we distance from a realist perspective, as we do not consider the state as the main object of our analysis. This approach enables us to treat individuals, people, as the ultimate moral recipients of our framework. We will disregard the harm that could be made to arbitrary entities like states, as the only measure of judgment will be the harm made to individuals. The harm made to other states is only relevant as long as their citizens are eventually harmed the consequences of that act.

How do we understand if an individual has been harmed or not? To do so, we need to identify a common set of values that satisfies two requirements: as Bellaby (2012)

puts it, these values have to be vital to the well being of the individual and they have to be vulnerable to external influences. These values should be vital because they would be would be fundamental for enabling individuals to pursue their own goals and aspirations, and any restriction or damage done to them would cause harm regardless of its consequences (Bellaby 2012). They should also be vulnerable to external influences, as any damage done to these values should not come as a consequence of the actions of the individual, but from circumstances outside of his control.

In his Theory of Justice, Rawls (1999) identified a comparable body of "social primary goods", such values being *things that every rational man is presumed to want*. Accordingly, such universal interests would be: fundamental rights and liberties, freedom of movement and free choice of occupation, political rights, income and wealth and the social basis of self-respect[9]. Feinberg (1987) instead identifies a similar body of interests, and distinguishes between welfare interests[10], which are minimal, and ulterior interests that related to people's interests and goals. It is important to note that these interests go beyond human rights: those are the things that every free and equal individual needs to pursue his rational plan of life, human rights included. As Rawls' conception of primary goods is fundamentally instrumental to his theory of distributive justice, Bellaby's conception of vital interests (and Feinberg's theory from which Bellaby's predates upon) is much more fit for our interest, as it answers the question: what are intelligence agencies not allowed to take away from people?

We then would not go too far from reality if we accept Bellaby's (2012) claim that, in-between these vital interests, the ones who are more likely to be subject to restrictions due to intelligence gathering activities would be the *individuals' physical and mental integrity,* along with *their autonomy, liberty, sense of self-worth and privacy*. It follows that any intelligence action that impairs one of these interests in

[9] Of course, this conception has endured some criticism, notably from Amartya Sen (1980) and his capabilities approach, for being too inflexible and not able to take into account the diversity of human beings

[10] "*Interests in the continuance for a foreseeable interval of one's life, and the interests in one's own physical health and vigor, the integrity and normal functioning of one's body, the absence of absorbing pain and suffering or grotesque disfigurement, minimal intellectual acuity, emotional stability, the absence of groundless anxieties and resentments, the capacity to engage normally in social intercourse and to enjoy and maintain friendships, at least minimal income and financial security, a tolerable social and physical environment, and a certain amount of freedom from interference and coercion*"

any way is therefore damaging other individuals, as it impairs their freedom. And it is clear that a moral obligation arises to prevent violation of these interests.

Moving again to the realm of laws, we find out that there is an overlap between laws and ethics when speaking about vital interests. As a matter of fact, such values are often embedded in the constitutional norms and laws of pretty much every country in the world, and are often recognised across the globe and codified in international law (as in the case of human rights). As we said, intelligence agencies, being governmental agencies, cannot violate the law of their country: their action has to be consistent with constitutional norms, laws and treaty obligations. Therefore, are there enough moral and legal boundaries for preventing agencies from breaching these fundamental human rights?

We are not ready to answer this question. Our considerations, up until now, do not tell us however whether or not this obligation not to hurt other people always holds. As we have seen, consequentialist approaches may allow harm to be done if the benefits outweigh the negative consequences. And we have already seen how legal limits can easily be breached by intelligence agencies. We still have no compelling moral reason to say why intelligence actions should always restrain themselves from damaging other people, or if exceptions can be made. We finally meet our conundrum. How do we reconcile the need to protect these rights with the national interest? And, most importantly, can the national interest provide a sufficient motivation to circumvent these limits?

7. Redefining national interest and national security

Since security services are here to assist in the protection of the national interest, the question of what is the national interest and who defines it becomes even more relevant. The two questions are deeply entangled with each other, and countless scholars have debated on the issue.

Within the realist tradition, Joseph S. Nye Jr. (1999), identified the national interest in a democratic system as *the set of interests widely shared by citizens in regard to their relations with the rest of the world*. Accordingly, this definition goes beyond strategic interests, and can include values such as democracy and human rights. This definition implies that a democratic definition of the national interest relies on public discussion and decision by legitimate institutions on the long-term shared interest of a community.

This conception is not undisputed. There are obvious issues with identifying who gets to decide the national interest. In Rousseau's concept of *volonté générale*, the general will could only be deduced from rationality itself. It was not the result of a compromise or even the deliberation of a majority, but rather the harmonic expression of popular will, detached from contingencies and individuality.

Others believe that, in all societies and throughout history, elites (were them political, economic, etc.) always detained control over the definition of national interest, having the power to define it better than everyone else. As far as in 1845, Marx defined the national interest as a superstructure, as "*each new class which puts itself in the place of one ruling before it is compelled [...] to represent its interest as the common interest of all members of society, that is [...] it has to give its ideas the form of universality, and present them as the only rational [...] ones*".

It is actually difficult to believe that a national interest can fully be based on public discussion and decisions by legitimate institutions. More recently, social constructivists like Wendt (1999) have put the emphasis on norms and shared values of the international arena. He acknowledges that states have an intrinsic interest in "life, liberty, property and collective self-esteem", but the national interest remains essentially a socio-cultural construct dictating nations' beliefs and behaviour. This body of norms and shared values is able to shape and embed a national interest within society much better than any public deliberation, which merely mirrors these values.

On second thought, this problem of who gets to decide the national interest is secondary for our intents and purposes. The problem is that this concept, as it is

usually defined, completely lacks any criteria for universality, pitting states one against each other simply in the reason of a poorly defined conception of common will. As Chuter (2011), argues, the argument for national interest is historically "shaky", precisely because these interest may often be in conflict with each other, periodically leading to tension and violence. A just and universal framework for intelligence cannot rely on this definition of national interest as its basis. But how can we transform a concept so deeply rooted to national contingencies into something universal?

We need to rethink the concept of national interest as a moral construct, detached from the historical and societal contingencies that came to produce it. In direct contrast with Morgenthau's (1949) realism, we will claim that yes, there are supra-national moral principles concrete enough to give guidance to the political actions of individual nations.

Rawls, in *A Theory of Justice* (1999), attempted to provide a definition of national interest anchored on a social contract. Accordingly (1999), under a veil of ignorance, the result of his hypothetical contract is that people would agree on two principles of justice: the so-called liberty principle and the difference and equal opportunities principle[11]. Both principles ultimately serve one true purpose: ensuring that each citizen has equal access to the primary goods that we mentioned before. Only in this way every individual will receive instrumentally valuable tools to achieve their goals in their lives. Therefore, according to Rawls, the national interest of a just state is defined by these two principles of justice. In order to better pursue its national interest, a nation *will aim above all to maintain and to preserve its just institutions and the conditions that make them possible (Rawls, 1999).*

Dwelling too much on Rawls' distributive justice conception goes beyond our scopes: Rawls' conception may be too much anchored on his theory of distributive justice. His social contract focuses on the distribution of primary goods, while we are

[11] First principle: each person is to have an equal right to the most extensive basic liberty compatible with a similar liberty for others

Second principle: social and economic inequalities should satisfy two conditions: (a) they are to be of the greatest benefit to the least-advantaged members of society (the difference principle) and (b) offices and positions should be open to all though principles of equality of opportunity

interested in the preservation of vital interests instead. We do not need a veil of ignorance to distribute these vital interests, as people are already found holding them. Rawls' thought is, nonetheless, a step in the right direction for our purposes. We want to value autonomy and equality of opportunities above everything else as well. We then agree that all the vital interest and the institutions put in place to safeguard them ultimately serve the purpose of ensuring that everyone can benefit from autonomy and equal opportunities, and there are few reasons not to believe that people would not agree on these vital interests being protected, regardless of their citizenship.

The national interest would then coincide with upholding and safeguarding these vital interests and protecting them from external threats. Therefore, as long as morals and laws concern these vital interests, concerns about ethics and legality are always in the national interest, and there are no reasons why these concerns should be overridden. Overriding them would be incoherent: why would you let your intelligence agency violate these principles – abroad and domestically – if you want to value these principles above everything else?

Also, we will argue that maintaining and preserving the institutions that are supposed to protect these vital interest is a vital interest in itself: put simply, the existence institutions that are unable or unwilling to ensure the protection of these interests can harm citizens directly, as the absence of these safeguards leaves them vulnerable to potential harm.

This conception of the national interest is clearly in contrast with the realist tradition, when Hans J. Morgenthau asserted in 1949 the primacy of the national interest over moral concerns: "*A nation should pour into the general principles of morality its own national conception of them, and then try to impose those moral principles, universal in form and national in content, upon the rest of mankind with fire and sword*".

Our reflections turn the realist position around: the national interest cannot provide a sufficient motivation to circumvent the moral – and legal – limits of intelligence, simply because these limits are there for the national interest. We are

assuming that, in our societies, people would hold their rights and their freedom in their highest regards. What is the point of national security if it hinders these interests?

This conception also implies a perspective shift on how the tasks of intelligence agencies are often portrayed. If we think of their objective as solely being responsible of "granting security" to the citizens, we are on the wrong way. Without referral to the vital interests, security is an empty word: we could as well be monkeys in a cage. Intelligence and security are the means to an end, but security is not the end on itself, the ends are the people and their vital interests, since that is the only national interest.

Finally, it could be argued that this conception leaves foreign citizens vulnerable to external threats, as only creates obligations domestically. We claim that, while the main objective of intelligence agencies is to protect their citizens' capacity to enjoy their vital interests, this has to be done with due respect to the vital interests of the citizens of other states. To do so, we could adopt some sort of veil of ignorance, and we could argue that these principles should not be violated abroad since we do not know whether we will be on the receiving end of these abuses or not. However, it will suffice to say that nations and agencies should respect a reciprocity clause when employing certain methods against foreign nationals: this is basically an application of the Golden Rule, in its negative form: *one should not treat others in ways that one would not like to be treated.*

These considerations on the Golden Rule give us the opportunity to move our framework further away from national contingencies. We have argued that the protection of vital interests is a vital – and national – interest in itself, and we have seen that agencies can harm these interests both domestically and abroad. Why would an innocent citizen be subject to abuses from intelligence services, when he did not consent to be treated this way?

We can expect some restrictions of these vital interests to still actually take place. There are probably people that, by consentingly participating in the world of national security, may *expect to be treated* in a certain way, even if they may not like it. There

are probably still some rights and freedoms that can be restricted, as long as there are individuals that are freely deciding them to put them at stake.

Otherwise, what use would intelligence agencies have?

8. A theory of consent as a basis for our framework

Consent, here, is the keyword. And, as Pfaff & Tiel (2004) put it, not only consent is ultimately the manifestation of our freedom of choice and action, but it is also the fundamental moral criterion for establishing a line of conduct towards other individuals. When a gambler consents to gamble his money on a horse race, he knows that there would not be any injustice in losing his money should his horse lose the race, as long as the race is not rigged. But if I did not gamble any money, it would not be just for me to pay for something I did not consent to be part of.

Intelligence, using lt. Mattox's (2002) allegory, is much like a football game. Everyone who joins a football game can join it either as a player or as a spectator. Just as the football players tackle each other, actions such deception, blackmail and other acts that may compromise a person's vital interests are all allowed between intelligence agents. But just as football player cannot tackle a spectator, an agent cannot use his power against a citizen. It all comes down, again, to consent.

Consent in "taking part in the game" implies, first of all, that the person making this choice actually had the freedom to do so. Autonomy is safeguarded in this framework in two ways: first, because an individual is free to pursue his own goals as long as his vital interests are safeguarded and, second, because an individual is free to choose whether or not risk them by entering the "national security game". But equality is also protected: people are not subjected to unequal treatment just because they detain specific information, but rather depending on how much the target has compromised himself by taking part in the intelligence world.

Consent, however, is just one element of the picture. While Pfaff focuses on consent as the sole determinant for distinguishing targets, we argue that shared expectations play an equivalent role in intelligence ethics. Only by knowing what to expect from other players and what other players could expect from her, an individual can truly and consensually decide whether to engage in the game or not. Shared expectations condition how people behave and they interact with each other. Agencies should not target citizens indiscriminately because these people do not expect agencies to behave like that and because agencies should not expect any harm from ordinary citizens. At the same time, ordinary citizens should avoid getting entangled in matters of national security when they can expect intelligence agencies to target them once they enter the game.

Consent in taking part in the game, along with shared expectations, contributes to shaping social roles. Roles allow for a much better and comprehensive identification of targets. The intuition here is that there are different kinds of players in the intelligence game, each one playing a different role and each one being allowed different – if none – restrictions of vital interests based on their consent and shared expectations. The criterion for what is morally acceptable and what is not changes depending on the role of each player. While similar, this is a far cry from Just War distinction between combatants and non-combatants. There are many more roles in intelligence and there is no size-fits-all way to approach to each actor.

Also, the premises are different from Just Intelligence approaches. We have no principle of just cause based on abstract national interests, but rather a body of rights and legitimate interests that have intrinsic value in a way that they both have to be promoted and preserved. The measure by which other people may be deprived of these rights and interests is proportional to the damage these people are willing to cause to other people's rights and interests by making themselves legitimate targets of intelligence. Here the distinction between targets and identification of their roles in intelligence is paramount, taking priority over anything else.

Also, thanks to this conception, we do not distinguish between nationals and foreigners, we do not make unrealistic calculations of aggregate welfare and we do not let definitive moral imperatives stopping our actions even if the target is

legitimate. This is a framework that can always work, as long as there is certainty over the complicity of each individual[12].

Of course, as we have just hinted, the world is far from being made of only players and spectators. Pfaff & Tiel (2004), list five different categories of targets, depending on "how much" the target is involved in the game and their level of consent. First, there is the ordinary citizen; second, we have the person possessing sensible information without being aware of its value; thirdly, there is the person in possession this information, aware of its value but unaware of being targeted; then, we have individuals in possession of information, aware of its value, aware of being targeted and willing to release the information; lastly, the fifth level is where the game changes, as here we have the malicious individual, recruited agent and the intelligence officer. Our conception of roles may comprise many more categories, but these ones just listed form a satisfactory abstraction.

In the first two cases, any kind of abuse or restriction of primary values directed directly towards these people, who are innocent in the sense that they did not agree to the rules of espionage, is unethical and unjustifiable under any circumstances. In these cases intelligence can only make use of open sources or non-intrusive non-harmful methods of collection. Even in the case of national emergency, nobody would ever agree on that. The third case is the tricky one, as some minor abuse - like deception or blackmailing - may be acceptable, as long as the target involved willingly took this responsibility when acquiring the information. They would have agreed, through their free will, to be part of the game.

The fourth case causes no concerns, as the target is well disposed to release the information and no harm is being made to him. It can be argued that when an officer buys information from an agent, this agent is doing a moral wrong by betraying his state. However, the moral responsibility to release this information only lies in the hands of the agent, who is consensually releasing this information in exchange for money and/or other goods. For what concerns the intelligence officer, as long as this

[12] And yes, this is exactly the weak point of this argument. Certainty is impossible to achieve, especially when individuals are targeted by agencies without respect to due process. Sure, compensation is imperative if an individual is unjustly targeted, but the existence of such risks imposes again on officers the moral obligation to limit the harm made to their targets as much as they can, even if they are suspected to fully participate in the intelligence process.

information is important to prevent harm to her national community and no harm is being made to the agent, no moral wrong is committed. The government acquiring this information, it could be argued, could use it to harm foreign nationals, but here the government has a moral obligation not to use this information in this way. This, however, applies to the whole profession, no matter how the information is acquired: if the officer and the agent have substantial evidence to believe that the officer's government will not respect this obligation, there are few doubts that this information should not be released.

In the last case, much more is allowed. Since this target is an individual who freely choose to be fully part of the game, Pfaff et al (2004) argue that, in this case, he may be subject to deception, incitement, bribery, blackmail - even with manufactured evidence - and appropriation. Of course, even here, there are limits to what can be done. As Bellaby (2012) claims, *all other things being equal, some interests such as physical and mental integrity can take precedence over the other interests such as autonomy, liberty, self-worth or privacy*. Torture, for example, may still pose as an ethical limit to intelligence gathering. It would be interesting to ask ourselves whether a terrorist withholding vital information that could safe other people's lives could be tortured during interrogation under this framework. The answer is not easy, while it is true that the collective commitment to protect these rights and goods gets hindered simply by torturing another person, it is also true that the individual expected this kind of treatment if he were to be captured and that his actions would have threatened the lives of other people.

In these cases, criteria of proportionality (and here we can use some help from just intelligence) should then help officers decide which methods to employ. Differently from just intelligence approaches, cost-benefit evaluations should not drive this decision, but should be rather driven by how much of our collective commitment towards respecting and promoting human dignity are we eager to give up by harming another person in order to protect other people from harm. This suggests that even action against another officer, agent and any other legitimate targets has to respond to some specific criteria for it to be ethical. As mentioned, agencies hold a moral obligation to limit the roughness of their methods to the strictly necessary, even against legitimate targets.

We now approach the end of our argument. Do our findings mean that ethical or legal concerns may be overridden in espionage? No, what we argued just means that the boundaries of what is ethical and what is not are different from time to time, because the rule of the game may be different. In no way, even because of a supposed national interest, an innocent citizen should be deprived of his vital interest. And, still, action should be as measured and as less harmful as possible even against legitimate targets. Going past those ethical boundaries would contradict the same national interest that those intelligence services are trying to protect.

One last remark: we have not gone into details. Under this model, some kind of non-coercive, non-harming intelligence gathering (better known as indiscriminate pre-emptive spying – IPS) could apparently still be permitted, but there is still no consensus on whether this kind of intelligence collection is something that violates vital interest or not. The problem with modern intelligence is that this kind of intelligence is seemingly getting more and more invasive both because of technological developments and for shifting perceptions of each one's sense of privacy. We will take a look at these concerns, and much more, in the next part of this study

---

Part II

Intelligence ethics in the digital age

1. Intelligence ethics in the digital age

Intelligence has not remained inert to technological development. Over the last few years, as a consequence of significant improvements in Internet connectivity, the change of the online habits of ordinary people and the capillary diffusion of devices capable of registering, storing and uploading data, we have witnessed a radical increase in the ways agencies can gather and analyse intelligence – and also act covertly.

Intelligence has been highly receptive to developments in big data analysis. These developments have enabled intelligence agencies to scale up their SIGINT practices significantly, coming in possession of potentially immense surveillance capabilities. These development lead us to question whether our previous considerations on intelligence ethics may still considered valid, as basic definition of consent and responsibility are definitely put into question due to a system of dispersed morality which characterized the digital arena.

Many commentators, such as Vaidhyanathan & Bulock (2014), have then perceived a shift in focus from foreign intelligence collection to mass surveillance in the field of national security. This claim, while not incorrect, may be misleading on some accounts: first, it may appear that surveillance and intelligence are two different things, leading us to question whether or not the previously explored ethical frameworks could be applied from the start; second, this claim may lead us to believe that modern – and digital – intelligence focuses solely on surveillance[13].

While it is true, as we will see later, that these technological developments have potentially created a Panopticon-like scenario, in reality, there is not much difference between the analytical categories of intelligence and surveillance. State surveillance is just a facet of intelligence, or rather a consequence of it. Using Lyon's definition (2007), we can identify surveillance as *the monitoring of the behaviour, activities, or other changing information, usually of people for the purpose of influencing,*

[13] Over the course of this dissertation, we will argue whether or not the previously explored ethical norms can still be applied to intelligence due to new technological developments. It comes without saying that, if we accept the misunderstanding that surveillance and intelligence are two different things and that modern intelligence is only made up of surveillance, the whole point of our argumentation would probably fall, as intelligence and surveillance would presumably stand to different ethical standards.

managing, directing, or protecting them. This notion is not incompatible with the definition of intelligence we have previously given, according to Chuter's definition (2011): surveillance still requires information secretly acquired from an entity, which that entity does not want you to have. Therefore, there are no reasons to argue that surveillance – *per se* – stands to different ethical standards to the one we have given for intelligence.

In second account, it is not true that intelligence has evolved solely in terms of surveillance. Intelligence is still being collected and analysed in many other ways, and surveillance is not the sole reason why intelligence is being collected. As we will also see later, NSA's hyper-controversial PRISM program was also primarily intended as an intelligence collection device directed towards foreign entities. The fears of mass surveillance appeared only later, when Edward Snowden exposed these methods.

The thing that has changed, maybe, is the way intelligence is being perceived by the general public in terms of integrity and accountability. This is precisely why the Snowden revelations are so important and why will be discussed extensively over the course of this second part of the dissertation. These revelations showed that technological developments have led intelligence to step far beyond its boundaries, bypassing consent when disregarding fundamental vital interests. This has raised obvious issues on the lack of institutional oversight of agencies and caused considerable damage the accountability of democratic institutions.

2. Big Data and hyper-connectivity

We cannot proceed with our analysis, however, without first analysing these technological developments and how they affect intelligence. What we call big data is a multi-layered process facilitated by technological developments in the field of ITCs, closely tied to the trend of hyper-connectivity that is characterizing the new millennium. This process has lead to a gargantuan increase in the amount of information produced by the network. The quantity of data uploaded has never been

so high and it is still growing exponentially. As the Zwitter (2014) reports, 5 billion gigabytes of raw data are now recorded every 10 seconds, against 10 minutes in 2013 and two days in 2011. In 2003, only the entire body of recorded history so far was as heavy as 5 billion gigabytes. The quantity and complexity of data is now far beyond any past level, so much to render traditional data processing applications obsolete.

Big data is more than just a quantitative increase in the amount of data produced, gathered and processed. What has also changed is the way this information is registered: it is not just the data that increased in quantity, but also the tools that are used to record it. As Vaidhyanathan and Bulock (2014) report, data is electronically gathered in many ways. Just to make a few examples, GPS devices – especially the ones on smartphones – are now able to record a trail of a person's movements, credit card transactions are similarly recorded, and cameras and microphones are now nearly ubiquitous (Vaidhyanathan & Bulock, 2014). But, most importantly, most people load their information on the internet by themselves: social networks, email services, forums, all these web platforms – and many others – store data that people willingly uploaded on them. As we will see later, this process is only bound to accelerate in the near future with the advent of the connected phenomenon of the Internet of Things, as each aspect of people's lives may be converted into data, a process that has now been called "datification" (Cukier, 2013).

Other qualities that make the big data phenomenon stand out from the past are the organic and global nature of the data collected. According to Zwitter (2014), big data is much more organic than statistical data and can capture people's lives and habits much better than surveys, questionnaires and other research instruments. Big data is also potentially global, inasmuch as the data can be collected from anywhere in the world, as long as there is some connection to the Internet. Big data is then able to capture the digital footprint of every person in the world much better than any other method used in the past.

This digital footprint is not easily cancelled, but it is rather stored under the form of data into servers that could be located anywhere in the world. Once the data is stored, it can then be processed by algorithms and then handed to human beings for interpreting them. There are many people and organizations making use of big data,

from researchers, advertisers to, obviously, intelligence officers. As we see, the word big data refers to this whole process of production, collection, and analysis, a process that mirrors the three categories of actors involved, as Zwitter (2014) lists them: big data generators, big data collectors, and big data utilizers.

Amongst these three stakeholders, generators are, literally, the entities that generate data: they sit at the first stage of the process and can either be people, natural phenomena or artificial actors. It is important to remember, in fact, that *not all data potentially falling into the category of Big Data is generated by humans or concerns human interaction* (Zwitter, 2014). Collectors, instead, govern the gathering of the data, choosing which data to collect and store, and for how long it is stored. Utilizers, instead, sit at the final stage of the process and can either produce more knowledge by bringing the datasets together or also influencing other people behaviour though this knowledge.

It is an irresistible process. From a "utilizer" standpoint, as Vaidhyanathan and Bulock (2014) put it, institutions have every incentive to make big data bigger. Big data helps researchers and universities to provide even stronger evidence to their Commercial, marketing and advertising services need big data to remain competitive. All agencies and organizations that rely on information for their work cannot resist the call of big data: this, obviously, includes intelligence agencies as well. Of course, this fascination, as the two authors put it, may be *driven by market fundamentalism and techno-fundamentalism*, and sure there are risk of oversimplifying the reality by equalizing correlations to causations, but it undeniable that big data provides some clear benefits to their ultimate users. The bombastic celebration of big data and its benefits has surely not provided any reason to put a check on its excesses so far.

Also, as Jonas (2015) argues, hyper-connectivity is irresistible to human "generators" as well: more and more products and services require customers to give their information away, even if in a private way. The choice – if there is a choice – not to make use of these products and services may be a difficult one for many, and may entail a certain degree of sacrifices from personal to professional.

How much does big data relate to intelligence, though? Big data is important because is transforming cyber-intelligence, a branch of SIGINT, both qualitatively and quantitatively. As Scott Applegate (2015) reports, cyber-intelligence relates only to the process of exploitation of the wider analytic category of cyber-warfare, which also encompasses disruption. The differences between the two are similar to the differences between intelligence analysis/collection and covert action: while exploitation activities are focused on exploiting information technologies to steal various forms of information and data, disruption is instead intended to deny, damage, disrupt or destroy information resources and their underlying architectures or other connected technologies (Applegate, 2015).

Cyber-intelligence then focuses on gathering – or stealing – and processing information through the means of ITs. Some early examples of cyber-espionage (a branch of cyber-intelligence) can be traced back to the actions of individual hackers stealing information from a state and selling it for profit to another one (Applegate, 2015). It has now evolved significantly, so much that the damage of cyber-espionage in 2013 ranged from 20 billions of dollars to 120 billions solely for the United States (Applegate, 2015).

With the advent of big data, cyber-intelligence has evolved significantly. Agencies can now track the movements, calls, transactions, and pretty much any other action of their targets. But big data also allows for profiling much more than single individuals, enabling the monitoring of whole communities. Much more controversial, however, are the opportunities opened by indiscriminate pre-emptive targeting: big data analysis allows for performing preliminary intelligence gathering (in order to determine the "legitimate" targets) on pretty much everyone. Linked to this process is also the blurring of borders between domestic and foreign intelligence, where cyber-espionage has blended with cyber-law-enforcement. Big data allows for targeting foreigners and nationals indiscriminately, and this, in practice, has also been facilitated by unclear legislation on the field. We will get back to these points later.

Intuitively, big data and, most importantly, the way it is exploited, pose many ethical difficulties. First, however, we need to delve into the recent NSA revelations to better contextualize the issue.

3. The Snowden Revelations

The implications of big data in intelligence have been made evident only recently. On June 2014, Edward Snowden, a National Security Agency contractor, and his confidant Glen Greenwalt released to the public, with the collaboration of international media outlets such as the Guardian and the Washington Post, a large amount of confidential data from the NSA. Most of this data was related to the so-called Verizon and PRISM affairs, and revealed massive surveillance programs conducted by the NSA and its Five Eyes partners[14] over the last years.

The Verizon affair was the first to be revealed. Accordingly, the NSA organized the collection of metadata of calls within the US and between the US and another country, with the collaboration of Verizon and other providers such as ATT and Sprint. Metadata does not show the content of the calls, but rather shows the number/IPs of the caller and the recipient, their location and other data that relates to the duration and the time of the call. This is does not mean that this data is not important: this is *data that can be mined, that can be mapped, that can be correlated with any other important data set* (Vaidhyanathan & Bulock, 2014), allowing for a much more invasive intrusion into a person's privacy.

Metadata is not innocuous from a privacy perspective: it enables the construction of a detailed profile of a person, and along with other data – such as financial transactions – it allows for identifying the habits and activities of said person, enabling the construction of her detailed profile (Miller & Walsh, 2016). Accessing another person's metadata can be as harmful as any other invasion of privacy.

[14] The Five Eyes, a group of countries with a tradition of collaboration in intelligence, are: the UK, the US, Australia, Canada and New Zealand.

Revelations on the PRISM affair shortly followed, and their impact was even more shocking on the public. It was revealed that agreements between NSA and US-based ITC companies such as Facebook, Google, Skype and many others took place, in order to obtain almost direct monitoring of the communications of their users (Vaidhyanathan & Bulock, 2014). This time PRISM also involved the interception of the content of communications other than the metadata.

It should be noted, however, that these acts – especially the PRISM affair – placed a new kind of spying into the spotlight: indiscriminate pre-emptive spying. Accordingly, targets were spied *en masse* on the basis of no prior intelligence, so to select suspected individuals (Travaglione, 2016). As Wisnewski (2016) describes it: with PRISM everyone is being spied upon, but no one is really doing the spying. Government agencies like the NSA have access to private information, such as religious beliefs, political views, etc., but for the most part, this information goes untouched and unseen. Could this be considered an invasion of privacy?

Many believe so. As Miller and Walsh (2016) describe it, these actions were a *major, indeed stunning, breach of institutional confidentiality*. The repercussions of these revelations were harsh, and the trust people put in their institutions has surely been thwarted. Undoubtedly, the way this surveillance was carried out was unprecedented both in its nature and scope (Wisnewski, 2016), and this has led many to believe the institutions that were supposed to protect their rights and interests were actually actively violating them and turning their state into a surveillance state.

However, the NSA is not the STASI and, by keeping its actions secret, it is obvious that the aim of the NSA was not to intimidate or control their citizens but, rather, to protect them, for better or worse. What has, however, led the NSA's officers to overextend so much beyond the ethical limits of their profession? As The Guardian (2013) reported, there are two trends that affected this unprecedented expansion of surveillance: *the fear of terrorism created by the 9/11 attacks and the digital revolution that led to an explosion in cell phone and internet use.* Developments in ITC and big data enabled NSA actions to be taken a step further, and the post 9/11

public debate was so imbued with the fear of terrorist attacks that the NSA felt security concerns could trump over privacy issues.

All of this was also facilitated by a perhaps too permissive legislation that resulted from an increasingly unclear demarcation between domestic and foreign intelligence. As a matter of fact, under the provisions of the US Patriot Act, law enforcement agencies were not subject to the national legislation – and judicial controls – on wiretapping but rather on the provisions of the FISA, the Foreign Intelligence Surveillance Act, which were much more lax (Miller & Walsh, 2016).

We have tried to provide some contexts to the main issues related to big data. Before going further, however, it is now opportune to ask ourselves what these issues are and how they can be approached from an ethical standpoint.

4. The issues with mass surveillance

Snowden's revelations opened the door for a wide number of concerns. The majority of commentators were concerned over the transition of democracies towards surveillance states, as we mentioned. Other related concerns focused on the rise of questionable practices such as predictive policing and pre-emptive justice. We can recognise these as the main contemporary fears of the use of big data in intelligence.

Concerning the fear of a surveillance state, Foucault's version of the Panopticon has been evoked quite often. The idea was first developed by English philosopher Jeremy Bentham, who envisioned the Panopticon as a prison with a peculiar design. Accordingly, the design consisted in a circular structure with cells for the prisoners around the perimeter and a room for the guards in the middle, which allowed for a single watchman to observe all the cells. The observer would have been able too see everything that happened in the prison (which is, literally, what the word "*Panopticon"* means) even if he could not see all the cells simultaneously. As a result

of this design, inmates would have refrained from misbehaving, as they were unable to know whether they were watched or not. The sole assumption of being watched was enough to ensure nobody misbehaved.

When Foucault, in 1975, revived the concept, the context was radically different, but the basic idea remained the same. The idea transitioned from an actual prison design to a philosophical metaphor for surveillance, as he described the modern state as a series of Panopticons. After the NSA revelations, many commentators have been led to believe that contemporary panopticism may be even more pervasive that Foucault believed (Wisnewski, 2016). Accordingly, technological innovation has only amplified these pre-existing panoctic structures, allowing for a nearly complete and invisible observation of society in which everyone can be watched without being allowed to know if they are. Vaidhyanathan & Bulock (2014), drawing from cryptography and its enormous influence in big data analysis, have also tried to give a name to this new kind of Panopticon, calling it "*Cryptopticon"*. Thanks to the global nature of big data, this Cryptopticon is potentially much stronger and pervasive than Foucault's version of the Panopticon as it can monitor pretty much everyone, everywhere. We will take the liberty to address this process as global panopticism.

Another issue related with the modern Panopticon is the fear of a "Minority report" effect – as this is the movie many commentators end up mentioning when raising this issue. We are using this term as an umbrella term to address concern related to the concepts of predictive policing and preventive justice. According to Zwitter (2014), predictive policing is already in place in a number of cities: in LA, for example, certain streets and areas are subject to more surveillance simply because crimes are more likely to happen in those areas. For what concerns pre-emptive justice, while some preventive measures may exist in certain legislations, this remains nonetheless a mainly philosophical concept, as we are still far from crossing the border of science fiction.

These concerns relate to the long-term socio-political consequences of indiscriminate spying. They voice some legitimate apprehensions about possible scenarios. We want, however, to focus more on the individual actions of the officers – or agencies – and see how these practices are wrong – and harmful – in the first

place. We then have to look for the qualities of NSA officers' behaviour that are wrong from a moral standpoint. Indeed, we need to better articulate these concerns in order to put them into an individual perspective. This perspective will also allow us to identify other ethical issues related with those data exploitation and intelligence gathering practices

Therefore, to see if the actions of these agencies are unjust in the first place, we have to look at how these actions directly impact on the lives of other people, harming not only their autonomy but also their sense of equality. To put it in our terms, we have to look at how these actions may impair their possibility to enjoy their vital interest. We will identify a few areas of controversy, which we will further investigate later so to establish whether or not people can be harmed from these practices.

First, some commentators argue that big data exploitation is generating new inequalities. There is basically a disadvantage between the watchers and the watched, as the inability to know if they are being surveilled or which data is being collected puts them at an ethical disadvantage, limiting their knowledge and autonomy (Zwitter, 2014). Accordingly, the actions of the watchers are morally wrong because they are creating a power imbalance between the different stakeholders in the big data process, limiting the autonomy of the people who do not have access to this kind of data. By putting other people inside a Panopticon, when they are not able to know if they are being observed or not, the watchers may erode the autonomy of the watched, harming them.

The challenge here will be to identify whether of not these new methods employed by intelligence agencies can hold from a moral standpoint. How are the watchers harming these people, what vital goods are they damaging? Some have tried to justify some of NSA's actions on the grounds that targets have given their informed consent in having their data treated in a certain way when they uploaded it. Therefore, can the watched be considered as legitimate targets, as they agreed to the terms and conditions of these web platforms? What makes a target legitimate, now? Also, if the Panopticon is invisible, and surveillance is harmless, can it still be considered

morally wrong? And, finally, how can intelligence still pursue its aims in the digital age if certain methods are considered morally inadmissible?

Other issues relate to the moral responsibility of the watchers: in an era where data collection and exploitation are mostly run by algorithms and when different actors intervene in the big data process, where does the moral agency of agencies and officers lie? Snowden's revelations also exposed issues on whistleblowing and officer responsibility: can Snowden's actions be considered good from an ethical standpoint? They did considerable institutional damage, and they may have put some people in danger if Snowden did not take the necessary precautions. Surely, the knowledge of being spied upon has surely influenced other people's lives, in a way that may have provoked harm to them. And surely, these revelations may have caused harm to national security, exposing NSA's methods and rendering them ineffective against the real *bad guys* they are supposed to target.

Finally, overreliance on big data may be problematic under a methodological perspective too: as Zwitter (2014) argues, *correlations suggest causations where there might be none* (Zwitter, 2014). Big data has an aura of scientific validity simply because of the velocity, volume, and variety of the phenomena it encompasses (Pasquale, 2015). But, by privileging quantity over quality, big data, if not supplemented by other meaningful knowledge, may have a distortive effect on reality, creating the risk for false positives and decontextualizing information. While we felt it was important to mention this last concern, we will not delve further into this specific methodological issue, as dealing with it more appropriately would go beyond the scope of our study.

5. Other connected trends

Technological progress does not go in a single direction. Along with the developments in big data analysis, there are many other new trends related with innovation that are affecting intelligence. All these trends are entangled together, affecting each other significantly: starting a discussion on intelligence ethics in the

digital age becomes, then, impossible without at least mentioning all these other trends and how they can influence each other.

5.1 Decline of "real-world" HUMINT

Probably one of the trends that is affecting intelligence the most is related to the slow decline of human intelligence against other disciplines such as SIGINT and OSINT. It is a process that, as Reed (2016) reports, has been going on for a long time. Accordingly, the American intelligence community, over the last two decades, has significantly scaled down the cost and effort put into human spies and their networks, in favour of SIGINT and other technological methods of intelligence gathering (Reed, 2016).

Technological advancements and, again, the rise of big data have only accelerated this process. Also, the IT revolution has also brought an "open source revolution" which carried its consequences onto the intelligence sector, to the point that OSINT is now projected to exceed the share of 80% of intelligence collected, as it expands into the realms of more traditional collection disciplines (Mercado, 2007).

Why is this important? This trend may be ethically problematic in many ways. First, the decline of HUMINT signifies the abandonment of a model of traditional discriminate targeting in favour of much more indiscriminate forms of targeting. Second, as Hu (2015) argues, it is not just HUMINT that is declining: even within SIGINT, small data surveillance is losing a tug-of-war against big data cyber-surveillance. The success of big data creates a self-reinforcing loop that only attracts more investments in SIGINT and OSINT, while also providing further justification for PRISM-like programs. It is the whole intelligence that is transitioning towards this brave new world of big data.

While "real-world" HUMINT is losing momentum, it is still true that human intelligence can still be collected online. Other than simply blackmailing agents by email, the proliferation of forums and online communities has opened new doors for infiltration and exploitation for intelligence. As Harris (2016) explains, the Joint

Threat Research Intelligence Group (JTRIG) – part of the US Government Communication Headquarters – has been allegedly involved in covertly profiling, infiltrating, distorting and discrediting of communities and individuals online. While the JTRIG has yet to confirm this allegations, this practice has raised, in the eyes of activists such as Glenn Greenwald (2014), many concerns: precisely, the ability of agencies to infiltrate and manipulate online discourse has been blamed for compromising the freedom and identity of the Internet itself. We will further analyse the ethical implications of online HUMINT later on in our study.

5.2 Automated intelligence

Linked to the decline of HUMINT, an increase of usage of software and robots in intelligence can be detected too. Machines and software in intelligence can either substitute of the human element (such is the cases of reconnaissance drones) or they can complement it (like algorithms in big data).

Emerging robotics technology, along with sophisticated software technology, are now seeing extensive military and intelligence operational history (Lin & Ford, 2016). Military robots have long been considered more effective than humans in fulfilling specific tasks. These tasks have usually been listed as the three Ds: dull, dirty and dangerous (Lin & Ford, 2016). Robots, having no fear, anger or emotions in general, have then proven themselves to be the perfect candidates for these kinds of tasks.

Robots are also used to gather intelligence. Civilian applications, for example, include experimentation of *K5 autonomous data machines* to monitor behaviour in public places (Lin & Ford, 2016). Unmanned Aerial Vehicles – commonly known as drones – are however the most widespread collection system. Their usage has not been restricted to military reconnaissance, as agencies such as the CIA have been known to use them extensively (Radsan & Murphy, 2011). The problem here is that distinction between military and intelligence gathering applications may be subtle – when non-existent at all. Many of these robots and drones are equipped with

weapons for defending themselves in case of attacks, and can switch from collection to attack almost instantly. The issue here is that armed attack and intelligence collection answer to different ethical standards, due to the exceptionality of the former. These principles may be difficult to reconcile when a platform can seamlessly perform both tasks.

This is not the only problem with drones: as their usage increases and their presence becomes more pervasive, one more drone in the sky may signify one more eye to invade other people's privacy. This makes robot a potential issue in the digital arena too: should they become another mean to collect information indiscriminately, they will probably only amplify the pervasiveness of global panopticism. What is interesting from our perspective is that these robots (such as the aforementioned K5 data machine) are able to record data without asking for consent. If we take in consideration recent developments in the Internet of Things and smart objects, this issue gets more and more pressing as the potential for these machines to monitor every aspect of our lives comes close to full realisation.

These considerations link with other developments in software technology, as a great share of work with big data analysis is now performed by algorithms and computer programs. As a matter of fact, Snowden revelations showed that the degree of monitoring put in place by the NSA would not have been possible without state-of-the-art data mining software allowing for bulk listening[15]. As The Intercept – the news website founded by Greenwalt himself – explained (see Froomkin, 2015), these programs were designed to *analyse and "extract" the content of voice conversations, and even use sophisticated algorithms to flag conversations of interest*. In the past, wiretapping was subjected to the physical limitations of having an actual person doing the listening, making discriminate targeting more of a necessity due to resource constraints than a moral requirement. Now, thanks to the aforementioned developments, this kind of software allows for a fully automated and nearly complete monitoring of telephone and digital conversations. This issue is ethically relevant inasmuch as this software and these algorithms enable the level of monitoring

[15] See the intercepted NSA newsletter "For media mining, the future is now!", available at: https://edwardsnowden.com/docs/docs/sidtoday-future-is-now-final.pdf

necessary to make global panopticism an actual possibility, surmounting the physical human limitations that previously ruled out this possibility.

Last but not least, innovation in software technology and robotics may raise a problem of responsibility, as they may deprive the officer of his own moral agency. Where does responsibility lie when software – or a robot – misbehave and harm other people? What if the intended and programmed behaviour is already morally dubious? Who is to blame, for example, when a computer programs wiretaps into other people's conversations: the programmer who wrote the code, the agency using it, or the websites and providers recording this information? These technological developments are leading to a problem of diffused moral agency, which we will address later.

5.3 Uncertain legal frameworks

It is important to remember that NSA's actions were not made under a regime of complete illegality. As Miller & Walsh (2016) explain, the NSA initiated its PRISM surveillance program in 2007, and received legal legitimation through the 2008 Amendment Act to the FISA (Foreign Intelligence Surveillance Act). This acts expressly bestowed the NSA with a legal basis for enacting its mass surveillance, allowing for warrantless wiretapping. The problem here is that these provisions were intended for protection against foreign threats, but NSA nonetheless could extend its surveillance over domestic targets. As if the moral foundations of NSA's work were not characterized by uncertainty already, the legal fuzziness between domestic and foreign intelligence has worked out in favour of much more invasive and indiscriminate practices.

A process of blurring of lines between domestic and foreign intelligence (and blending of espionage with law-enforcement) can then be noted. This is not only the consequence of the changes occurred in the profession: it is the nature of its targets that is different from the past. In a post-9/11 world, contemporary intelligence targets have evolved into international and multi-actor threats that operate on

multiple areas. Terrorist groups such as the ISIL can be classified as threats both internally and externally, as their ramifications extend can far beyond state borders. As foreign intelligence gathering blends with law-enforcement (Miller and Walsh, 2016), it is inevitable that some uncertainty has arisen over what kind of legal framework should be governing the activities of intelligence agencies, and that the most permissive one was then adopted.

5.4 User adoption of privacy-protection tools

There is then one last trend that is worth mentioning. As a reaction to Snowden's revelations, a surge in popularity in privacy-by-design technologies can be detected (McDonald, 2015). As the name suggests, these are products and services that incorporate privacy protection into their overall design (Schaar, 2010). Some of recent examples include instant messaging services based on end-to-end encryption like Telegram (and, more recently, Whatsapp); the privacy-focused and non-personalised search engine Duckduckgo; and the onion routing web browser Tor, which enables encrypted and anonymous network communication. These – mostly – open-source and free tools are born out of hacktivism and can be considered as a way to defy the Panopticon; in the minds of many, at least.

Reception of these technologies has been mixed. While, as a result of the NSA revelations, 45% of Americans have changed their online habits in some way, it is also true that adoption of these technologies has not reached meaningful levels yet (McDonald, 2015). Some services with bad reputation – like the Tor browser[16] – have not seen widespread adoption. Others such as Duckduckgo, offering a user-friendly interface and clear incentives for privacy, have instead seen a decent increase in popularity over the last years (but are still far from reaching the market share of IT giants such as Google) (McDonald, 2015).

[16] Which has been know for hosting dedicated child-pornography websites and online marketplaces for weapons and drugs dealing

This trend, however, is still interesting in a variety of ways. These privacy-by-design technologies have the potential to rule out any kind of mass intrusion, rendering any kind of PRISM style surveillance virtually impossible. From an ethical point of view, these technologies are interesting because they can provide an alternative to other "irresistible" services and websites, encouraging users to make informed choices about their privacy, meaning that some form of consent can now be traced. It is worth questioning whether this alternative is actually viable or not, or if the now limited success of these technologies depends on the persistence of barriers to adoption, lack of interest in privacy issues or simply irresistible nature of mainstream services and technologies.

However, these technologies could also be used for malicious means: by rendering impossible to intercept communications, these technologies may actually rule out even more traditional and morally acceptable ways of gathering intelligence such as discriminate reactive targeting. Telegram, for example, *has become known as a preferred means of communication for the Sunni terror group ISIS, and was used by the ISIS cell that plotted the Paris terror attacks in November,* as the CNN reports[17]. It is an issue that cannot be ignored.

6. Testing our framework with the realities of contemporary intelligence

Now that the main trends and practices in digital intelligence have been identified, we are ready to analyse how these developments may be problematic from an ethical standpoint. Following our framework, we will see if certain practices in intelligence can be considered acceptable based on what harm they cause, who they target, and what responsibility do agencies and officers have.

Our analysis will start from where we left, at the end of the first part: observing that indiscriminate targeting practices can be harmless if kept secret, we will

[17] See http://edition.cnn.com/2016/08/01/europe/france-church-attack-telegram/index.html

question whether these harmless wrongs can be considered ethically acceptable under our premises. The analysis will then begin by questioning whether or not these new targeting practices have the potential to violate the vital interests we defined in the first part of the thesis and if, consequently, can also undermine people's autonomy and equal opportunities.

Secondly, the analysis will analyse the basis of consent in the big data process. Previously, consent has been valued as the cornerstone of our framework: consent in "taking part" in the intelligence game allowed for certain vital interest to be violated, depending on the role played and the degree of involvement, as actors shared mutual expectations on each other's behaviour. The focus will then shift on whether or not the basis for consent has now been eroded, and if it is possible to develop a new system of *infraethics*[18] in the digital age.

Lastly, our considerations will focus on officers' responsibility in particular. The Snowden affair will resurface again, as the individual responsibility of officers and the systemic consequences of whistleblowing – especially in terms of accountability – will be discussed.

7. Indiscriminate targeting and harm to others

When investigating how new intelligence gathering techniques can harm other people, looking at what vital interests can be hindered by intelligence activities could be a safe approach, as we did in the first part of this dissertation. There are few doubts that privacy is the one that is most endangered interests. While our societies hold privacy as one of their highest values, it is still true that some invasions of privacy have often been tolerated and justified on moral grounds. Spying has always implied, in some way, breaching a barrier of privacy, confidentiality or secrecy.

Discriminate reactive spying (DRS), as Travaglione (2016) defines it, is the practice of *spying on specific individuals or groups on the basis of prior intelligence, in order to verify some specific suspicions or to accumulate more evidence*. This is

[18] See Floridi's (2013) definition of infraethics later

the way intelligence gathering is traditionally understood, and this practice has also been widely accepted and used for law enforcement and criminal investigations for a long time, provided that it has received the approval of competent judicial authorities. Using our approach, this method only harms the privacy of specific people who are reasonably suspected to pose a threat to national security (by endangering other people's fundamental rights and interests).

Recent developments in big data gathering and analysis, as we have seen, have however given rise to a new practice: indiscriminate pre-emptive spying (IPS). Here, this practices allows for *spying indiscriminate targets en masse on the basis of no prior intelligence, in order to identify suspect individuals* (Travaglione, 2016). This is the kind of spying that characterized NSA's PRISM program. IPS targets are supposed to be innocent, and this is why this practice is ethically dubious. There is no argument of reasonable suspicion: IPS targets are not targeted because they have made themselves a threat for other people, as data mining is supposed to discover suspect behavioural patterns or suspect communication networks among *ex ante* unsuspected targets (Travaglione, 2016). The great majority of the people targeted are no players in the intelligence game.

Technological developments, especially with the breakthrough of Big Data, have led intelligence gathering and analysis to a quantitative and qualitative leap, offering new and more effective means of surveillance. Snowden revelations have only made the issue more pressing. IPS has obvious implications for the privacy of citizens. We consider privacy a vital interest – using, again, Bellaby's terminology – specifically because people cannot fully exercise their autonomy without. Using Rawls' definition of primary goods, privacy can be considered as part of the body of fundamental rights and liberties that, in conjunction with the other goods, allow citizens to feel free and equal, along with developing a sense of justice and a conception of good.

This being considered, is this invasion of privacy justifiable in terms of security? And, most of all, can it be considered harmful? We have already rejected Kantian moral absolutism: it is possible to harm another person, as long as this person has made itself a legitimate target.

Under our framework, distinction between targets is paramount. Agencies have no right to indiscriminately harm citizens, no matter their nationality or where they are residing. However, if those acts cause no harm to citizens, we should see no reason to reject them. This may seem like the case for IPS: as Wisnewski (2016) reports, there is evidence that autonomy and privacy are mediated through belief. Accordingly, an individual may not see her autonomy impaired in any way and act inhibited, as long she believes his privacy was not violated, no matter if she was constantly monitored and surveilled.

This leads us to question whether it is possible to wrong people without directly harming them. Travaglione (2016) calls the theory that holds that harmless wrongs are possible "pure-wrongism". This is a concept introduced in 1988 by Joel Feinberg in *Harmless Wrongdoing*, his final volume of his magnum opus *The Moral Limits of the Criminal Law*. Feinberg however maintained that, with the exception of a few special cases, legal coercion could not be justified when no harm or offence to others has been made. Travaglione also rules pure-wrongism out, for the sake of his argument. We could argue that IPS may be acceptable if really harmless but, in order for it to be so, there is one necessary condition to satisfy: it has to remain secret. If the mass surveillance system is discovered, as it happened with PRISM, serious harm to people's autonomy may be done, creating a Panopticon situation where people are restraining themselves because of the fear of being watched.

PRISM-style spying, however, cannot be considered to be entirely harmless, even if it remains secret. When agencies monitor citizens indiscriminately, they are still violating a vital interest (or primary good), a violation that could potentially cause harm if discovered. Privacy, a vital interest, is violated, and since it is an institution supposed to protect it that is violating it, damage is being done to the integrity of the whole institutional system. Harm is done to citizens indirectly since the integrity of the institutional system put in place to protect their vital interests is itself a vital interest for the community. The institutions risk becoming morally corrupt, because they are here to protect a common good such as privacy and are actively violating it, going against the national interest and harming its own community. These institutions are also supposed to share commitment towards respecting these interest everywhere, no matter the nationality of the targets: under the reciprocity

clause, if you do not want another state to wiretap into you, you should not want your state to do the same to other citizens too.

But, most of all, this kind of spying creates knowledge asymmetries, actively creating inequalities even if the targets are unaware of it. PRISM-like system create a significant power imbalance within a society, as the watchers can know everything about their targets, while the watched cannot even know if they are being spied upon. This creates systemic inequalities that are, again, harmful in general and undesirable for the national interest, in the sense that this system privileges a form of knowledge available only to those with access to costly resources and technologies (Andrejevic, 2014), de-empowering anyone else and consequently damaging democratic institutions.

But let us put these considerations aside and suppose that democratic institutions are not causing harm to their integrity by indiscriminately violating the privacy of their citizens, as long as they manage to keep their activities secret, as we suggested earlier. As Travaglione (2016) argues, this is the condition of "perfect voyeurism", and it is the first of two conditions for allowing IPS when rejecting presumptions of moral absolutism and non-wrongism. According to the author, from a strictly consequentialist standpoint, undetected voyeurism cannot be considered morally objectionable (as long as moral absolutism and non-wrongism are excluded), as it causes no harm to its victims. Therefore, intelligence agencies, when performing IPS, they should ensure it to remain *undiscovered, unpublicised and unexploited,* for it to be morally justifiable.

However, according to Travaglione (2016), there is another condition that must be satisfied, and this is the condition of necessity. Accordingly, the moral presumption against invading privacy should be defeated only when security, the good provided by IPS, offsets it. This means that IPS must be causally efficient, proportionate and there must be no other less costly alternative (last resort). Travaglione here basically uses snippets from the intelligence war theory approach to define a set of criteria for necessity. We will avoid criticizing on these points on the basis of our previous considerations on adaptations of Just War theory to intelligence, for now, it will suffice to say that the fact that these criteria have to be used in order to justify IPS

suggests us that IPS is an exceptional instrument that cannot be routinely used by intelligence agencies. Causal efficiency, however, is the only element that matters here.

This being said, even if we accept that IPS is morally admissible only when these two conditions are satisfied, there is a problem that cannot be overcome. As Travaglione argues, there is a paradox between the perfect voyeurism and necessity conditions, as both can never be satisfied simultaneously (Travaglione, 2016). As he argues, for IPS to be causally efficient it must be exploited; it if is exploited, however, the possibility of IPS to be detected and publicized increases, compromising the perfect voyeurism condition. Moreover, for IPS to be perfectly voyeuristic, it cannot be exploited, but if IPS does not lead to any concrete usage, it cannot even be treated as necessary.

The only criticism here may be exploitation may not necessarily entail publicity. As the Snowden revelations have proven, once exploited, IPS is pretty difficult to hide; but let us go a step further and suppose that there is a way governments can actually use IPS while successfully keeping it secret. This is an interesting issue: if IPS regimes actually prevent terrorist attacks or other threats, how can institutions justify the interception of the suspected groups and individuals? As Travaglione argues, *the only way to keep IPS secret would be to thwart the process of free public information*. This, however, harms again the accountability of democratic institutions, as citizens are kept unaware of what their state is doing.

If, to this criticism, we add back the aforementioned issues of inequality and institutional integrity, we have enough motivations to argue that IPS is morally objectionable in many respects. However, there is still one significant objection to our reasoning, coming precisely from the consent-based approach we adopted. As we know, IPS targeting would not possible without all the recent developments in big data; more specifically, without everyone being so hyper-connected, the NSA would not have had any person to target. Could it then be that all these people, even if surveilled indiscriminately, are all legitimately targeted since they agreed to their information to be used in a certain way when using certain products and services? This leads us to another problem: what does consent mean in the digital age? What

makes a target legitimate in the digital age? Is everyone a "player" in the intelligence game now?

8. The basis of consent in the digital age

There is then one objection that can be made to the previous argumentation: these targets may all be legitimate since they explicitly gave their consent for their information to be shared when they signed up on Facebook, Gmail and similar websites and services, and hence they may *have voluntarily give up any right to privacy they once had* (Wisnewski, 2016). After all, before using most of these services and products, users are often required to agree to terms and conditions that expressly state that their information may be used for advertising, market research and other purposes.

It could be argued that big data gatherers were also expected to collaborate with the government for security purposes: refusal to co-operate for matters falling under the FISA umbrella would undoubtedly have been considered treason, as Yahoo CEO Marissa Mayer argued in the aftermath of the Snowden revelations[19]. It is not surprising then, that someone may claim that users gave their *informed consent* for big data collectors to gather their data and use it in a certain way when they started using these products and services.

The reality, however, is that normal people have barely any say when it comes to how their information is treated. This is the main problem: the basis of consent is eroded because moral agency, as Zwitter (2014) argues, is precisely dispersed.

[19] See here for a full interview http://www.businessinsider.com/marissa-mayer-its-treason-to-ignore-the-nsa-2013-9?IR=T

Before going further, it is important to better define what conditions govern moral agency. Here we will adopt Noorman's (2012) approach. Accordingly, moral agency is defined by three innate conditions based on free will and individualism[20]:

1- Causality: *An agent can be held responsible if the ethically relevant result is an outcome of its actions*
2- Knowledge: *An agent can be blamed for the result of its actions if it had (or should have had) knowledge of the consequences of its actions*
3- Choice: *An agent can be blamed for the result if it had the liberty to choose an alternative without greater harm for itself* (Zwitter, 2014)

Generally speaking, if one of these criteria is missing, the individual cannot be held fully responsible for his actions. Big data, however, challenges the concept of individual moral agency, making us question what free will and individualism can be found in a hyper-connected society. More precisely, it is debatable whether the *knowledge* and *choice* principles are satisfied.

The notion of informed consent is not entirely convincing, for at least two reasons. First, it is debatable how informed this consent is. It is undeniable that people rarely look at terms and conditions of use, and it follows that, if the users are not entirely aware of the consequences of their action, we cannot make them entirely accountable for these results and big data utilizers cannot use this information in a way that could harm them. There is, basically, a lack of *knowledge* that prevents them from fully exercising their moral agency. It could also be argued that, even when consent is informed, people do not expect or consent to the government using this information (Wisnewski, 2016) and, despite the data being already public, no one really considers suddenly being the subject of research in Twitter or Facebook studies (Zwitter, 2014).

It is true, however, that we all should have looked at the terms and conditions of these services (even if pretty much nobody does it): from a legal standpoint and according to US supreme court "third party doctrine" (as reported by Wisnewski, 2016), people lose any reasonable expectation of privacy when they disclose it to third parties, no matter whether they looked at the terms of conditions or not. This

[20] Mind it: the term "agent" used in the following definitions is not to be interpreted in the intelligence connotation of the term

does not change that there is probably not enough clarity and awareness yet on how big data utilizers use people's data, and that nobody probably expected to be indiscriminately targeted in a PRISM-style surveillance program. It could be argued that people deserved to know that they could have been targeted indiscriminately and that the information should have been conveyed with more clarity when they signed up to these services, and this puts the acts of NSA and ITC companies in a fuzzy moral ground.

But there is also an even better argument against the theory of informed consent. Even if people were fully informed about the way their information was going to be used, we can argue that users did not have much *choice* anyway. People use these products and services for a wide number of reasons: there are clear benefits for using these products, as there are clear disadvantages for not using them when everyone else is. By keeping them out of social media or other services, people miss out on social interaction and many other opportunities. For example, many may miss out on job opportunities coming from Linkedin, while others, like musicians, artists or even people running local businesses may also actually lose money by not having any Internet presence. This suggests us that the price to separate oneself from society may actually be too high, and that people do actually harm themselves by choosing not to "go digital". Some may be fully aware of the potential loss of privacy, but the lack of alternatives prevents these people from making an independent choice. As Tulloch (2016) puts is, the *entwining of the self and the social with digital technologies is irresistible*. There usually is no choice but *hyper-connectivity*.

It could be argued that emerging privacy-by-design technologies may help create an alternative and give some choice to the users. This, unfortunately, all depends on whether or not these technologies manage to surpass most of the barriers to adoption their faced with. As McDonald (2016) explains, lack of obvious incentives, lack of knowledge on the existence of privacy-enhancing tools, difficult installations procedures and bad user experiences can hinder the adoption of these technologies. In some case, some barriers may be surmountable. Duckduckgo, fuelled by the PRISM controversy, has managed to carve a decent share of market, overcoming 10mln search queries per day on June 2016[21].

[21] Data available on https://duckduckgo.com/traffic.html

Still, this is a paltry achievement when compared to the 3 billions searches on Google search. In other cases, also, there may not be any alternative at all, due to the monopolistic nature of established IT products and services. While these monopolies may not last forever, as Haucap & Heimeshoff argue (2013) and as evidenced by the downfall of Myspace, it is undeniable that these services – social networks especially – tend to concentrate all users over the same website. There is no point in using Telegram as long as anyone else uses Whatsapp, as there is no point on coming back to Myspace when all your friends are using Facebook. This, again, makes adoption of mainstream services almost irresistible, severely limiting autonomy and choice of the users.

Also, and most importantly, information may now be uploaded online even without the consent of the individual, even if no consent was given. Jonas (2015) reports two trends that are leading to bypassing consent: first, the development of the Internet of Things (IoT), and second, acquaintances and friends inadvertently handing over the data of another person.

The Internet of Things is a relatively recent phenomenon. This process relates to the ensemble of common household products – nicknamed *smart objects* – that are enhanced by electronic devices to provide local intelligence and are then interconnected in a network through the Internet (Kopetz, 2011), so that they can interact with humans or other smart objects. Smartphones are one of the first examples of these products. Apps like Google Maps, for example, interacting with a smartphone's GPS, are now able to track the user's daily movements with precision and conserve them in its history, which can be accessed remotely. Many more products are now entering the market, such as smart refrigerators that can keep track of expiry dates of food; vehicles that can diagnose malfunctions or even drive by themselves; and so on. What is new about the IoT is not only the disruptiveness of these objects, but most of all their pervasive deployment (Kopetz, 2011).

The problem here is that these products can monitor a person habits as closely as ever, and that this information is stored online in centralized servers that are probably located hundreds of miles away from us. This is information that can be

accessed by big data utilizers, and intelligence agencies specifically. The advent of more products offering even further inter-connectivity is inevitable, and their adoption nearly irresistible as they replace other more traditional objects (Jonas, 2015).

The Internet of Things is only bound to complicate consent even more: as Peppet (2014) explains, some smart objects have *no means to confront a user with a privacy policy or secure consent* simply because they lack physical input buttons (and the terms and conditions may be buried somewhere on the Internet). Also, these objects challenge current conceptions of privacy as the data they gather may be meaningless when taken alone: this sensor and biometric data usually does not constitute personal information, so few precautions for privacy may be taken, and no notice for consumer consent may be presented at all (Peppet, 2014). However, when data from different object is taken together and linked to a specific person, here all this data acquire huge meaning painting allowing for a near perfect profiling of a person. If we hold our privacy to our highest regards, the only choice left here is probably abstaining from using these products.

But in other cases, even with all the due caution, personal information may still be given away. Such is the case of third parties providing your information, inadvertently or not (Jonas, 2015). Some personal information may be on public records, like property ownership, but other information may be inadvertently uploaded by friends and acquaintances. An individual's number, address, and other personal information may be present on different systems, and this information may have been uploaded online on social networking websites and other online services (Jonas, 2015). Again, with the development of the Internet of Things, information pertaining to us may even end up being recorded by objects belonging to our friends and acquaintances too, without us giving any consent.

Hyper connectivity looks then irresistible, and consent may be completely pulverised. If the conditions for users to make free and informed choices about their online activities are missing (because they had no choice or knowledge), as it seems to be the case here, these targets cannot be considerate legitimate. We then need to rethink consent in the light of the introduction of these technologies; otherwise these

people will continue to be morally wronged by agencies such as the NSA due to these fundamental misunderstandings.

8.1 Potential objections to our argument

There are, however, a couple of final objections that can be moved towards our considerations on consent.

The first argument may be that, as Wisnewski (2016) argues, the Snowden revelations have actually created the conditions for informed consent, spreading *knowledge* about how the data is used, and since people are still using this technology, they are apparently consenting to their data being collected. This is an interesting argument: maybe, as effect of hyper-connectivity, people are not that much interested in their privacy anymore, or simply they believe they can still exert some control over the data they generate. Still, this argument tells us that people may now have the *knowledge* to expect certain consequences from their actions, but not that they now have a *choice*. Apathy to these matters could then be a valid explanation for continued usage of these products and services, but we can shrug this argument off pretty easily if we take into account our observations on the irresistibility of hyper-connectivity.

The second case is related to the concept of democratic consent: according to Wisnewski (2016), intrusion into privacy may be justified provided that *1) there are mechanisms through which citizens may revoke their consent to said intrusions; and 2) citizens do not use these mechanisms to revoke their consent*. This argument basically claims that authorities can be held accountable for their actions and that the only way people can consent is through democratic discussion and deliberation, so that they can express their *choice*. Of course, another pair of necessary conditions for this system to work is that 1) citizens are aware of the actions of their government and 2) the democratic mechanism is functional.

Surveillance, however, cannot work if people know exactly how their information is used and taken, otherwise, there would be no reason to announce this invasion of privacy, as malicious individuals may as well circumvent these controls rendering the specific collection process useless (as Wisnewski, 2016, argues). Even if they do not know how or when, they still know that surveillance is going on. Put in other words, this argument claims that citizens may actually tolerate Panopticism if they feel that state surveillance actually works out in their favour.

This argument, however, is ethically problematic under many accounts. First, democratic mechanisms should be used the last line of the defence against abuse from the government, not as the only one, as the fundamental values such as privacy should not be violated in the first place. Second, even if a majority has consents with this kind of intrusion, this does not change the privacy of a minority of people who did not consent would still be violated. Privacy is a fundamental good and this minority is being harmed, as their concerns about security do not offset their concerns about privacy.

The final, and most important, counter-argument, however, is that this theory of democratic consent only works for domestic intelligence and, in this specific case, the US, as is the only state that exerts some form of legislative control over the NSA and big data giants. Foreign states and nationals do not have any control at all, even if their citizens democratically revoke their consent, as foreign agencies such as the NSA can still monitor their conversation with the complicity of Internet companies.

9. Discriminate targeting practices and harm to others

According to our observations, we can safely claim that indiscriminate intelligence gathering practices such as IPS are wrong on many accounts. Discriminate practices (both HUMINT and SIGINT), however, have not remained uncontroversial. Hyper-connectivity has led to the proliferation of online communities, and online HUMINT, especially through the actions of the JTRIG – which manipulated and infiltrated

online groups – has been blamed for hindering online freedom. This process has been aided by big data analysis too, enabling near perfect profiling of targeted groups and individuals. Can these concerns be considered legitimate?

There is, however, nothing inherently wrong with discriminate targeting practices. If officers infiltrate groups selectively, they are doing no wrong: if these people have consciously made themselves a threat to other people, there is nothing wrong in deceiving them or invading their privacy. The problem here is more subtle: how can we identify a certain behaviour as threatening on the in the Internet? And how much harm is allowed?

Due to the networked nature of the Internet and thanks to the proliferation of online communities, it is difficult to determine with precision what individuals or groups can be considered threats to national security. Does simply visiting a forum where extremist ideas are shared makes you a threat to national security? And what about being friends on Facebook with suspicious individuals? Internet multiplies the connections we have with other people or groups, making each one of us a potential target.

Also, due to hyper-connectivity, collateral damage scenarios may be severely amplified: targeting a specific group may damage other people too. As Zwitter (2014) argues, *the nature of hyper-networked societies exacerbates the collateral damage caused by actions within this network*. The risk is that practices that are too invasive may really hinder online discourse generating the false perception that all social networks, forums and online boards have been infiltrated in a Panopticon-like scenario. This may cause harm to many people by hindering their autonomy, so we want to avoid this scenario at all costs.

For this reason, online discriminate reactive spying needs clear limits for its actions. The moral compass for evaluating online HUMINT and SIGINT can only be based on the legitimacy of their targets. Our first issue is that entities targeted are not solely individuals but also whole groups and communities: here malicious individuals may coexist with completely innocent people, with the risk of harming them too if these groups are targeted. The main problem here will be identifying the

element that makes a certain group a threat. How can we have a reasonable suspicion that this group is dangerous?

Harris (2006), inspired from Vattimo's distinction between strong thought and weak thought, comes in our aid. He argues that only individuals and communities which exhibit "strong thought" that endangers vital interests and the institutions put in place to protect them, and that this targeting does not endanger internet freedom. Put simply, these groups and individuals can be targeted because of the context of their conversations.

Targeting these groups does not degrade the integrity of online discourse precisely because the values of these groups are against a society that nurtures values of freedom and privacy. Drawing from Vattimo, physical violence feeds on metaphysical violence, and cannot exist without it. As Harris adds (2016), *certain beliefs and thoughts can be violent through their capacity to exclude others and to close down debate – a way that is incompatible with genuine democracy*. Just as like Popper (1945) argued that we should reserve the right not to tolerate the intolerants, we can claim that agencies have a duty to monitor, infiltrate and even distort and discredit[22] groups and individuals who can endanger democratic values and the vital interest of other people with their ideas. Other groups and communities, knowing they are exercising their freedom of speech with due respect to the vital interest of the others, can thrive safely in the knowledge that they are not going to be targeted.

Accordingly, groups such as religious fanatics and political extremists (and Harris adds conspiracy theorists) can all be targeted, as the ideas they express are violent, exclusionary and overall incompatible with democracy and vital interests of other people. So far, according to one of Snowden's leaks[23], the JTRIG has allegedly been targeting specific individuals (such as suspect caught in-theatre or cyber criminal), groups (Islamic extremists or those engaged in online credit card fraud), the general population (Iranians), or regimes (Zimbabwe African National Union – Patriotic Front). It is clear that, thanks to our considerations, the targeting the Iranian

[22] Turning intelligence collection into covert action
[23] See Dhami (2011)

population should not have be allowed in any way, but the other targets are all clearly legitimate.

However, as mentioned before, each individual within these communities may fit different roles in the intelligence game, ranging from the sympathizer to the malicious individual that may actually be willing to harm other people (using Pfaff's categorization[24], members of these communities may fit the first to the fifth category). This means that the most appropriate methods should be decided on a case-to-case basis, and that, again it is advisable to use the adopt, for the whole community, methods that can be considered acceptable for the lowest level of participation. Also, means should be proportionate to the value of the information being gathered: massive privacy intrusions cannot be allowed on the whole community if the importance of the information is trivial. Mindful of potential knock-on effects and that his actions may do more harm than required, some restraint is then required from the officer's part. Perhaps, then, the only information that should be gathered from these sources is whether or not the profile of certain individuals should be further investigated. Basically, the existence for these groups allows for a form of preliminary intelligence gathering that can help identify legitimate targets.

The problem here is that this may be technically difficult when identities are anonymized or hidden behind avatars, proxies and so on. The development of encrypted and anonymous technologies (such as Tor, Telegram and others privacy-by-design techs), reinforced by Snowden's revelations on IPS practices, may have indirectly damaged the ability of agencies to conduct discriminate collection practices, and even their ability to act covertly. As such, it is probably difficult to believe that malicious individuals may actually use traditional and not encrypted means of online communications for enacting their plans, especially when so many more safe technologies and protocols are available to them: indeed, we already argued how ISIS cells in France managed to circumvent the monitoring simply by using Telegram. In these cases, the real risk is that what is left of online HUMINT may simply be the profiling, infiltrating, distorting and discrediting of harmless groups and individuals with weird ideas.

[24] See Part I, paragraph 8

10. Officer's responsibility and dispersion of moral agency

The framework we have used so far is intrinsically based on officers' individual moral agency[25]. This is true for all the approaches analysed: in each of them, while the agency and the government may preserve a degree of political responsibility for the actions of their officers, the moral responsibility for the harm made to others only lies in the hands of the latter. If abuses in intelligence are committed, only the agency can be blamed for that.

Realist approaches (and just intelligence to a certain degree) may be the only exception, as the *Raison d'État* trumps over any other individual moral consideration. However, these frameworks still concentrate agency within the same entity: be it a Machiavellian prince, the intelligence officer or a group of individuals, there is always somebody that is morally accountable for the consequences of the spying profession.

As Reed (2016) argues, officers are not automatons. In traditional intelligence, officers are not merely obeying orders, but exert a wide degree of control over their actions. In HUMINT, for example, agents are pretty much free to decide the way they manage their agents. Should they resort to blackmail them and other forms of intimidation? Should they buy their loyalty with money? There are many ways officers can exert their discretion, and some of them are less morally acceptable than others.

With big data analysis, this kind of discretion disappears from the hand of the officer. Data is processed by sophisticated computer programs and then handed to the officer: the officer cannot decide how much or how selectively he is going to invade someone else's privacy. Most importantly, however, recent developments in

[25] For other general considerations of moral agency, especially on the dimensions of knowledge, choice and causality, go back to paragraph 8, page 80

big data analysis and the decline of "real-world" HUMINT, however, have led to a process of dispersion of moral agency that has eroded the responsibility intelligence officers and agencies, bringing the *problem of many hands* in intelligence. Using the definition of van de Poel et al. (2015), we can provide a definition of the problem of many hands as "*the occurrence of the situation in which the collective can reasonably be held morally responsible for an outcome, whereas none of the individuals can reasonably be held morally responsible for that outcome"*.

With the advent of big data in intelligence, some (such as Zwitter, 2014) have claimed that a similar system of distributed morality has developed. The ability of the actors to fully make moral judgments based on some notion of right and wrong and to be fully held accountable for these actions is then questioned. Where does the responsibility lie when personal data is gathered and privacy is breached? Is it the fault of IT companies taking this information from the users? Or is it rather the fault of intelligence agencies lawfully requesting this information? Or simply, as we have seen, users not properly reading the terms or conditions? Moral agency then gets dispersed amongst the units of a network and nobody is really responsible for anything: big data generators, collectors and utilizers they all seem to have their share of responsibility. Even the legislator could be blamed for allowing this kind of scenario.

This is a problem that spreads to automation in intelligence too: the diffusion of robots and automated analysis in intelligence raises the problem of who is morally and legally responsible for their actions when they harm someone else. As Lin and Ford (2016) ask, no matter whether harm is caused accidentally or intentionally, the autonomy of such robots and programs leads to questions about who (or what) is responsible for their actions. *Can we attribute responsibility to the robot itself or should we hold the operator responsible (or perhaps even the programmer)* (Lin and Ford, 2016)*?* Or even the agency commissioning them?

Going back to big data analysis, the problem is that, looking at the three conditions for moral agency (Causality, Knowledge and Choice), the three actors involved in the big data process – and, more concretely, in the PRISM controversy – can be found either deprived of these conditions (such as the case of missing choice and knowledge

for big data generators, as we have seen) or sharing the responsibility for many decisions. Looking at indiscriminate pre-emptive spying, we could argue, for example, that big data collectors (IT companies like Google, Facebook, Yahoo, etc.) have diminished control over the causality condition, because the ethically relevant result is only partially an outcome of their actions: collectors were the ones storing the information, but not the one uploading. Also, collectors did not have full control over their choices either: sure, they were the ones collecting the information, but they did not have the liberty to choose not to give the information to the NSA without greater harm for themselves (which, in this case, means being charged for treason). Similarly, agencies such as the NSA were the ones analysing this information, but not the one storing it or uploading it: they have the most responsibility here, because they had the knowledge and the liberty to act freely, but it should be noted that they cannot be found in full control of the causality condition.

Ultimately, the problem comes full circle once we take into consideration that this whole process spurs from the lack of knowledge and choice in the hands of big data generators. This is not to say that collectors and utilizers have no responsibility, but simply that their wrongdoings are spurring from an evident lack of autonomy that is lying at the beginning of the big data process, precisely when users upload their information. This is important because this confusion hinders agencies from exercising restraints in their profession. The problem here is that as long that agencies and web platforms assume that consent was given, it could be argued that no wrong was made both morally and legally.

But here we have already seen that consent was not given fully, as the conditions for informed consent do not hold. Responsibilities are chained together in what Zwitter (2014) defines as *dependent agency* (because the capacity to act is always dependent on another actor), but the whole system is based on ethically shaky foundations that nurture inequalities in the information age. The big data process is flawed simply because generators cannot fully exercise their liberty online and do not have control over their data; nevertheless, because of the implicit assumption that they can fully exert their autonomy, agencies feel morally allowed to use of this data.

We can take our analysis further and claim that the whole traditional system of shared expectations collapsed when intelligence moved to the digital realm. Using Floridi's (2013) conception of *infraethics*, we can argue that the *framework of implicit expectations, attitudes, and practices that can facilitate and promote morally good decisions and actions* has lost meaning in the digital arena. There are conflicting conceptions amongst actors of trust, respect, reliability, privacy, transparency, freedom of expression, openness (which Floridi all lists as moral enablers for infraethics), leading to contradicting expectations and morally bad outcomes. The only solution to this conundrum is reforming the system of infraethics by introducing new *moral enablers* (and enforcing pre-existing ones) so to reduce bad unintended consequences and spur a virtuous cycle amongst all actors, while defusing and removing all the *moral hinderers*.

11. Whistleblowing and accountability

Snowden revelations have also brought attention to one final issue linked to individual moral agency. As we mentioned earlier, officers are far from simply automatons. While there may be some "cowboys" or unscrupulous individuals longing for easy professional advancement, the majority of officers is made up of people with a sense of morality and professional integrity, as Reed argues (2016). While recent trends, as we have argued, have contributed to deprive officers of her responsibility, officers still hold moral obligations towards their country and their targets. How should an officer behave if he knew that his agencies and his fellow officers were not respecting their obligations, and harming other people, how should they act?

This is the same dilemma Snowden was faced with: should he have leaked these documents? He felt that NSA actions were violating fundamental rights and liberties, so he leaked them and yet, for exposing these illegitimate practices, he is now confined to Russia as twenty-one other countries refused his asylum-application (Travaglione, 2016).

Of course, it could be argued that Snowden's actions did more harm than good. First, Snowden could have caused harm to national security. The ability of the government to protect the vital interests of its population may have been hindered by these revelations. It is true, however, as Wisnewski (2016) reports, that Snowden handed his documents to the media, which, before releasing them, consulted the government about what should not have been released for matters of national security. Nonetheless, it could still be argued that, by releasing this information, Snowden rendered practices such as IPS ineffective, even simply by making malicious individuals look for other more secure communication tools.

Also, as we have seen, the more hidden surveillance is, the more it can ensure national security without creating a Panopticon scenario. Exposing the surveillance programs, he may actually have contributed to the creation of a global Panopticon, limiting people's autonomy and amplifying the harmful potential of PRISM-style surveillance. Travaglione (2016) argues that this could be another argument against indiscriminate surveillance: it is a *morally corrupting* practice that *turns a virtue into a vice*. Publicly denouncing illegitimate government practices that go against its obligations towards its citizens massively violating vital interests should be a laudable act, if not a moral imperative. With the case of clandestine mass surveillance, however, revealing these practices corrupts the original intention.

However, by leaking this material to the press, Snowden may have provided the basis for informed consent, as Wisnewski (2016) argues. People may be now made aware of the consequences of their online behaviour, and may now use more caution when giving away their information to big data giants. This, at least, could give a little more control to people when it concerns to the knowledge element of moral agency. This however, hardly gives full autonomy to big data generators (nor legitimacy on NSA's actions) since the irresistible nature of hyper-connectivity severely restricts the alternatives and choices they have.

However, while normal people may still lack the ability to choose due to the irresistibility of these technologies, leaking may still play a fundamental role for accountability. By leaking these practices, governments and agencies were put in a

position where they could have been held accountable for their actions. Indeed, not revealing these practices could be as much as harmful for democracy, whose integrity, as we argued, is a vital interest in itself. Do not people deserve to know what their government and intelligence agencies are up to, especially if these actions involve citizens directly?

As Lowenthal (2015) puts it, what can an officer do when something fundamental is at stake, when neither compromise nor silence is possible? The options are limited: the officer can either *struggle from within the system* or quit and possibly publicly denounce this behaviour. Sometimes agencies provide ombudsmen for sorting these issues internally, but in other cases there is not much choice between staying silent or exposing the agency. Whistleblowing, in these cases, becomes the only mean of protections against intelligence abuses.

We have to think whistleblowing in a systemic perspective, as it may be fundamental for accountability. As we know, it is inevitable that the actions of intelligence agencies have to be kept secret. So who watches the watchmen? We can only rely on the officers themselves, and especially more morally minded ones: if the actions of an agency are crossing a line, a way to denounce these acts should be granted, first though some form of ombudsman, and second through some form of whistleblowing. The leaker should not be considered a traitor as long he denounces certain practices and not specific people (with the risk of endangering them).

The point is that if an agency is crossing a line and harming other people and their vital interests, it is the agency itself that is betraying its obligations towards its people. This is true even if it harms foreign citizens: under a veil of secrecy, we would not want an agency to harm foreign citizens as we do not know whether we will be on the receiving end of the abuse or not. Accepting whistleblowing may then have virtuous consequences on the system. Agencies, knowing that their officers could defect and denounce their bad practices, would probably restrain themselves from employing methods that could be considered unethical. Whistleblowing may then become a moral enabler for building a virtuous system of infraethics, using Floridi's (2013) terminology.

Surely, this may be difficult to accept for many governments, and we do not know if this system would work well in practice and what unintended consequences it may lead to. Undoubtedly, looking at the Snowden affair, we know that intense debate on a potential NSA reform has taken place. The resonance of these revelations cannot be ignored considering they are potentially leading to institutional change. Even if this debate leads to nothing concrete, there are few doubts that, without Snowden, we would not have had the opportunity to question the morality and viability of the system of infraethics we have put in place for the digital space.

Conclusions

In this study, we have attempted to provide a comprehensive overview of intelligence ethics, with regards to both traditional and digital intelligence collection and analysis practices. Looking at the most recent developments in Big Data, we have seen not only how intelligence has evolved over the years, but also how the ethical issues related to it have transformed accordingly.

We have first provided an overview of existing approaches to intelligence ethics issues, including attempts to adapt Just War theory to intelligence. We have based our final framework on a social contract between citizens, arguing that people would find the work of intelligence agencies acceptable as long as these agencies do not cause direct harm (to national and foreign citizens as well) by violating a body of vital interests. These interests are to be safeguarded since they ultimately empower people with autonomy and equal opportunities, which we regard as the highest values in our framework.

This does not mean that these interest cannot be violated in any way: due to their autonomy, people can actually take part in the intelligence game (with the possibility of posing some form of threat to national security) and, depending on their level of involvement, some form of violation against them may be permitted. Maintaining some elements from Just Intelligence approaches, we argued that criteria of proportionality should be followed before engaging other players.

Recent developments, however, have shifted this feeble equilibrium in intelligence in favour of agencies, as technological developments in the field of big data analysis (linked with other trends such as hyper-connectivity) have bestowed agencies with a nearly limitless power to monitor every individual indiscriminately. We have argued that, from an ethical perspective, this trend has led to the undesirable development of a Panopticon, in which not only equal opportunities are damaged because of the implicit power balance between big data utilizers and generators, but also people's autonomy is hampered because of the fear of being monitored in any moment.

This scenario in which liberty and equal opportunities are diminished may, however, seem justifiable if we argued that people consented to this kind of surveillance and that these practices, if kept secret, do not harm innocent people in any way. What we have found, however, is that both of these assumptions do not hold in reality precisely because 1) users do not enjoy full moral agency when they give their data away and 2) harmless indiscriminate spying is impossible to obtain since it cannot be kept secret and unexploited at the same time.

The problem, however, is that neither agencies nor agents can be found to have full moral agency is the big data process. Hyper-connectivity has shaped a system of diffused responsibility that, without a shared system of infraethics, has opened the room for many abuses in intelligence collection. Intelligence agencies have now found themselves in a situation similar to Marlowe's Doctor Faustus. They want to achieve total knowledge, and they are getting close to achieving it, but this bargain with the devil comes with the price of corrupting agencies themselves. They end up harming other people, but they have no systemic incentive for not doing so.

The nature of intelligence and the secrecy of its practices makes impossible for these abuses to be subject to public scrutiny and feedback. We have argued, then, that whistleblowing may then become the last safeguard against abuses in intelligence. However, in intelligence, this is a behaviour that most likely equates to treason: the lack of possibilities to denounce abuses in intelligence provides then no incentives to curb excesses. This severely damages democratic institutions in terms of accountability.

So what? Do we accept intelligence for what it is? Not all is lost. Snowden revelations have opened a window for public discussion on intelligence ethics once again. This can help raise awareness on these issues, clarifying and cementing a set of ethical norms and shared expectations that can help reform intelligence practices. Hyper-connectivity and datification of our lives may be irresistible, but the Panopticon is still far from inevitable.

Bibliography

Agamben, Giorgio (2013); Stato di eccezione; Bollati Boringhieri editore s.r.l., Torino

Andrejevic, Mark (2014); Big data, big Questions: The big data divide; International Journal of Communication, 8, 1673-1689.

Applegate, Scott (2015); Cyber Conflict: Disruption and Exploitation in the Digital Age; in Lemieux, Frederic (ed.) (2015); Current and Emerging Trends in Cyber Operations; Palgrave Macmillan UK

Aquinas, T.; 'From Summa Theologiae' in Chris Brown, Terry Nardin and Nicholas Rengger (eds.) International Relations in Political Thought (Cambridge: Cambridge University Press 2002) p.214.

Archard, David, 2013, "Dirty Hands and the Complicity of the Democratic Public", *Ethical Theory and Moral Practice*, 16: 777–79

Arrigo, J. M. (2000); Military and Civilian Perspectives on the Ethics of Intelligence; Report on a Workshop at the Department of Philosophy, Claremont Graduate University

Bellaby, R. (2012); *What's the Harm? The Ethics of Intelligence Collection*; Intelligence and National Security, 27:1

Berendt, B.; Büchler, M.; Rockwell, G. (2015); Is it research or is it spying? Thinking-through ethics in Big Data AI and other knowledge sciences

Bronk, Christopher; Monk, Cody & Villaneson, John (2012); The Dark Side of Cyber Finance; Survival: Global Politics and Strategy

Bybee, J.S. (2002), 'Memorandum for Alberto R. Gonzales Counsel to the President', U.S. Department Justice Office of Legal Counsel, 1 August 2002, 5http://www.washington post.com/wp-srv/nation/documents/dojinterrogationmemo20020801.pdf4

Canon, D.; Intelligence and Ethics: The Cia's Covert Operations

Caimona, Michael (2007); Ethical Continuum, Consequentialist Approach to Intelligence Collection

Chomeau, John B.; Rudolph, Anne C. (2006); Intelligence Collection and Analysis, Dilemmas and Decision; in Goldman J. (ed.) (2006); The Ethics of Spying; Scarecrow Press

Chuter, David (2011); Governing and Managing the Defence Sector, Institute for Security Studies, Chapter 8, « Intelligence »

Clark, Robert M. (2003), Intelligence Analysis: A Target-Centric Approach 14- 26

Cockburn, Andrew Mark, (2012) The Ethics of State Security; Available at SSRN: http://ssrn.com/abstract=2090083 or http://dx.doi.org/10.2139/ssrn.2090083

Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment New York, 10 December 1984, partecipants, signatures and ratifications https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-9&chapter=4&lang=en

Cukier K. (2013); Kenneth Cukier (data editor, The Economist) speaks about Big Data; Available at: https://www.youtu- be.com/watch?v1⁄4R-bypPCIE9g (accessed 17 August 2016)

Dhami, Mandeep K. (2011); Behavioural Science Support for JTRIG'S Effects and Online HUMINT Operations; posted on The Intercept; Available at: https://theintercept.com/document/2015/06/22/behavioural-science-support-jtrig/

Doolittle J. (1954), Report on the Covert Activities of the Central Intelligence Agency

Feinberg, Joel (1987; 1988); Moral Limits of the Criminal Law: Vol.1 Harm to Others, Vol.4 Harmless Wrongdoing

Floridi, L. (2013) Distributed morality in an information society. Science and Engineering Ethics 19(3): 727–743

Floridi, L. (2009) Network ethics: information and business ethics in a networked society. Journal of Business Ethics 90: 649–659.

Forsythe, D. P. (1992); Democracy, war and covert action; Journal of Peace Research, vol. 29, no.4, pp. 385-395

Foucault, (1975), Discipline & Punish: the Birth of the Prison; Random House Inc. 1995

Froomkin, Dan (2015); The Computers Are Listening; The Intercept; Available at: https://theintercept.com/2015/05/05/nsa-speech-recognition-snowden-searchable-text/

Gendron, Angela (2005); Just War, Just Intelligence: An Ethical Framework for Foreign Espionage, International Journal of Intelligence and Counter Intelligence, 18:3, 398-434, DOI: 10.1080/08850600590945399

Greenwald, Glenn (2014); How covert agents infiltrate the internet to manipulate, deceive, and destroy reputations; The Intercept; available at: https://theintercept.com/2014/02/24/jtrig-manipulation/

Hu, Margaret (2015); Small Data Surveillance v. Big Data Cybersurveillance; Washington & Lee Legal Studies Paper No. 2016-6; http://dx.doi.org/10.2139/ssrn.2731344

The Guardian (2013); The NSA files. World News, the Guardian; Available at: http://www.theguardian.com/ world/the-nsa-files (accessed 18 August 2016)

Harris, Matthew (2016); The limits of intelligence gathering: Gianni Vattino and the need to monitor “violent” thinkers; in Galliott, Jai and Reed, Warren (ed.) (2016); Ethics and the Future of Spying, technology, national security and intelligence collection; Routledge

Haucap, Justus; Heimeshoff, Ulrich (2013); Google, Facebook, Amazon, eBay: Is the internet driving competition or market monopolization?; DICE Discussion Paper, No. 83, ISBN 978-3-86304-082-6

Hribar, Gašper; Podbregar, Iztok & Ivanuša, Teodora (2014); *OSINT: A "Grey Zone"?;* International Journal of Intelligence and CounterIntelligence, 27:3, 529-549

Hulnick, Arthur S. (2002); The Downside of Open Source Intelligence; International Journal of Intelligence and CounterIntelligence; 15:4; 565-579

Johnston, Rob (2005); Analytic Culture in the US Intelligence Community: An Ethnographic Study; Center for the Study of Intelligence, Central Intelligence Agency Washington; available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/analytic-culture-in-the-u-s-intelligence-community/analytic_culture_report.pdf

Jonas, Jeff (2015); The surveillance society and transparent you; in Rotenberg, Marc; Horwitz, Julia and Scott, Jeramie (ed.) (2015); Privacy in the Modern Age, the search for solutions; The New Press

Kopetz, Hermann (2011). Internet of things; Real-time systems (pp. 307-323); Springer, US

Lyon, David (2007); Surveillance Studies: An Overview; Cambridge: Polity Press

Lin, Patrick & Ford, Shannon (2016); The ethics of robots in national intelligence activities; in Galliott, Jai and Reed, Warren (ed.) (2016); Ethics and the Future of Spying, technology, national security and intelligence collection; Routledge

Lowenthal, Mark M. (2014); Intelligence: From Secrets to Policy, sixth edition; CQ Press

Mattox, M. (2002); The Moral Limits of Military Deception; Journal of Military Ethics 5:12

Mayer-Schonberger V. and Cukier K. (2013) Big Data: A Revolution that Will Transform How We Live, Work, and Think. Boston: Houghton Mifflin Harcourt

McDonald, Aleecia M. (2015); When self-help helps: user adoption of privacy technologies; in Rotenberg, Marc; Horwitz, Julia and Scott, Jeramie (ed.) (2015); Privacy in the Modern Age, the search for solutions; The New Press

Mercado, Stephen C. (2007); Sailing the Sea of OSINT in the Information Age, a Venerable Source in a New Era; available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html

Michael, Gabriel J. (2013); Anarchy and property rights in the virtual world; George Washington University

Michaels, Jon D. (2008) All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror

Miller, Seumas & Walsh, Patrick (2016); The NSA leaks, Edward Snowden, and the ethics and accountability of intelligence collection; in Galliott, Jai and Reed, Warren (ed.) (2016); Ethics and the Future of Spying, technology, national security and intelligence collection; Routledge

Miller R.B. (1991), Interpretations of Conflict, Ethics, Pacifism and the Just War Tradition (Chicago, IL; London: University of Chicago Press 1991)

Morgenthau, Hans (1949); The Primacy of the National Interest; The National Interest and Moral Principles in Foreign Policy; The American Scholar

Nye, Joseph S. Jr. (1999), National Interest in the Information Age; Annual Morgenthau Memorial Lecture Series (1981-2006)

Noorman, M. (2012); Computing and moral responsibility; in: Zalta EN (ed) The Stanford Encyclopedia of Philosophy

Parliamentary Assembly of the Council of Europe (Strasbourg, 23 June 2005); Democratic Oversight of the Security Sector in Member States, Recommendation 1713

Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs (Strasbourg, 11 June 2007); Secret Detentions and Illegal Transfers of Detainees by Council of Europe Member States Doc.11302

Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights (Strasbourg, 21 April 2015); Mass surveillance, Resolution 2045

Pasquale, Frank (2015); Privacy, autonomy and internet platforms; in Rotenberg, Marc; Horwitz, Julia and Scott, Jeramie (ed.) (2015); Privacy in the Modern Age, the search for solutions; The New Press

Peppet, Scott R. (2014); Regulating the Internet of Things: First steps toward managing discrimination, privacy, security and consent; Tex. L. Rev., 93, 85.

Sir Omand David; Phythian, Mark (2013); Ethics and Intelligence: A Debate; International Journal of Intelligence and CounterIntelligence, 26:1

Sir Omand, David (2007); The Dilemmas of Using Secret Intelligence for Public Security in Peter Hennessy (ed.) The New Protective State: Government, Intelligence and Terrorism (London: Continuum 2007) p.165

Perry, D. (1995); "Repugnant Philosophy": Ethics, Espionage, and Covert Action, Journal of Conflict Studies

Pfaff, T. (2006); Bungee Jumping off the Moral Highground: The Ethics of Espionage in the Modern Age; in Ethics of Spying: A Reader for the Intelligence Professional, ed. Jan Goldman (2006); Lanham, MD: Scarecrow Press

Pfaff, T.; Tiel, J. R. (2004); *The ethics of espionage*; Journal of Military Ethics, 3:14

van de Poel, Ibo; Royakkers, Lambèr and Zwart, Sjoerd D. (2015); Moral Responsibility and the Problem of Many Hands; Routledge

Rawls, J. (1999); *A Theory of Justice, 2nd Edition;* Harvard University Press

Radsan, AJ; Murphy (2011); Measure Twice, Shoot Once: Higher Care for Cia-Targeted Killing; Univ. Ill. Law Rev.:1201–1241

Reed, Warren (2016); Conclusion: A spy's perspective; in in Galliott, Jai and Reed, Warren (ed.) (2016); Ethics and the Future of Spying, technology, national security and intelligence collection; Routledge

Schaar, Peter (2010); Privacy by Design; Identity in the Information Society, 2010, Volume 3, Number 2, Page 267

Sen, A. K. (*1980*); "Equality of What?" in McMurrin (ed.), Tanner Lectures on Human Values; Cambridge: Cambridge University Press

Steele, Robert David (2007); in Johnson, Loch; Handbook of Intelligence Studies

Steinberg, Jonathan (2014); The Ethical Use of Unethical Human Research; Rutgers Journal of Bioethics; available at http://bioethics.as.nyu.edu/docs/IO/30171/Steinberg.HumanResearch.pdf

Taguba A. (2004), Article 15-6 Investigation of the 800th Military Police Brigade [The Taguba Report] p.17 x8, 5http://www.npr.org/iraq/2004/prison_abuse_report.pdf4 (accessed 26 May 2016)

Travaglione, Nicolas (2016); A dilemma for indiscriminate pre-emptive spying; in Galliott, Jai and Reed, Warren (ed.) (2016); Ethics and the Future of Spying, technology, national security and intelligence collection; Routledge

Tulloch, John (2016); Risk and Hyperconnectivity: Media and Memories of Neoliberalism; Oxford University Press

Vaidhyanathan, Siva & Bulock, Chris (2014) Knowledge and Dignity in the Era of "Big Data", The Serials Librarian, 66:1-4, 49-64, DOI: 10.1080/0361526X.2014.879805

Warner, Michael (2002) Wanted: A Definition of "Intelligence", 46:3; Studies in Intelligence, available at http://www.cia.gov/csi/studies/vol46no3/article02.html

Wendt, A. (1999); Social Theory of International Politics; Cambridge University Press

Wheaton, Kristan J. and Beerbower, Michael T. (2006), Towards a New Definition of Intelligence, Stanford Law & Policy Review available at https://journals.law.stanford.edu/sites/default/files/stanford-law-policy-review/print/2006/04/wheaton_beerbower_17_stan._l._poly_rev._319.pdf

Wisnewski, Jeremy (2016); Wikileaks and whistleblowing; in Galliott, Jai and Reed, Warren (ed.) (2016); Ethics and the Future of Spying, technology, national security and intelligence collection; Routledge

Zwitter, A. (2014); Big Data Ethics; Big Data & Society; 1: DOI: 10.1177/2053951714559253

Summary

Part I: Developing an ethical framework for conventional intelligence action

Using David Chuter's definition (2011), we can define intelligence as *the process of acquiring and making use of information from an entity - not necessarily a state - which that entity does not want you to have, without them realising you have acquired it*.

By definition, any intelligence agency will, sooner or later, face the inevitability of the moral dilemmas in their job. After all *the use of secret agents - voluntary and non-voluntary - is intended to provide valuable information believed to be unobtainable* (Perry, 1995). Where conventional methods fail in the task of retrieving such information, here intelligence agencies step into the game.

Of course, intelligence gathering is not always unethical or illegal. But, for its nature, there are cases in which the lines are blurred, or in which the morality of an action is disputable, at best. As president Eisenhower explained in 1954, justifying these methods entailed a *fundamentally repugnant philosophy*.

Such morality, however, is far from being universally considered acceptable, generating much public controversy over the last few years. After 9/11, cases of human rights violation, torture and inhumane degrading treatment for the purposes of intelligence collection – such as the ones occurred in the Guantanamo Bay detention camp - have not gone unnoticed, and more recent cases such as the release of the Snowden Archives have fuelled even more controversy, as new technologies provide agencies with nearly unlimited power to monitor conversations and store personal data. Consequently, recent controversy has generated criticism much more vocal than in the past.

All these abuses however were not committed for their own sake: intelligence communities face a tension created by the *duty to protect a political community* and

the reality that intelligence collection (and intelligence action in general) *may entail activities that negatively affect individuals,* as Bellaby (2012) argues. Many have tried to solve this tension by providing different moral frameworks for intelligence: needless to say, there is hardly any agreement here.

All three functional areas of intelligence (Intelligence Collection, Analysis and Covert Action) face their own dilemmas. While analysis and covert action too pose some significant controversies, intelligence collection will be the main focus of this study. Looking at HUMINT (human intelligence) collection, controversy has tended to focus on the topic of intelligence collection through interrogations, at least over the last decade. Think of other much discussed uses of torture and inhumane degrading treatment for intelligence gathering purposes. The Guantanamo case has surely made everyone aware of such issues: waterboarding and many other violating practices[26] were commonly used during interrogations, with the not-so-tacit approval of the government, as the – at the time – George W. Bush administration attempted to legitimize these activities through the 2002 *Bybee Memos*, which tried to redefine the very notion of torture as defined under the "Convention against torture and other cruel and inhuman degrading treatment or punishment", restricting it only to activities could have caused *serious physical injury* (limiting it to organ failure, impairment of bodily function, or even death) *or mental harm that would prove to last months or even years* (Bellaby, 2012).

There is much more than torture, as standard HUMINT collection tactics usually entail manipulation, coercion and deception. An officer must be ready to bribe, blackmail and manufacture evidence in order to obtain information from his sources. As Perry (1995) reports, CIA officials admitted that agents were often recruited through bribery or blackmail. Also, maintaining a cover can easily lead to immoral behaviour. Think of an agent disguised as a terrorist in a terrorist cell, gathering information on their movements and long-term plans. As Lowenthal (2014)

[26] As Bellaby (2012) reports, those other tactics included: *breaking chemical lights and pouring the phosphoric liquid on detainees; pouring cold water on naked detainees; beating with rope; sodomising a detainee with a chemical light and a broom stick; and using military working dogs to frighten and intimidate; hooding, hand cuffing with flexi-cuffs, beatings, slapping, punching, kicking; being paraded round outside the cells naked; exposure to loud noise; and prolonged exposure to intense sun over several hours; and even forcing a prisoner to masturbate in front of jeering captors*

arguments, there are areas like terrorism and narcotics in which intelligence collection relies heavily on human contacts: contacts must be developed with criminal organizations so as to enable successful penetration in the organization. Sooner or later, agencies and officers may be obliged to engage in unethical, criminal behaviour, in order not to blow their cover up. Could all these actions be justified in the light of a common, higher good?

Moving back to the realm of SIGINT (signals intelligence), recent developments in information and surveillance technology have bestowed agencies with a nearly unlimited power to monitor conversations and store personal data. The revelations coming from the Snowden Archives have shown how the recent technological developments have led to a quantitative and qualitative breakthrough in Signals Intelligence. Was this kind of intrusion into other people's privacy justifiable under a matter of security?

Of course, attempts to embed intelligence action within a moral compass have been made. As with any other human activity, many have tried to adapt intelligence into existing moral frameworks, with varying degrees of success. Literature seems to focus on a limited number of popular approaches: the nihilist, the realist, the utilitarian and the idealist. Just war theory has also been applied to intelligence.

Probably the most common – and apparently successful – approach to intelligence ethics is the attempt to adapt the Just War framework to intelligence. This approach has then become known as Just Intelligence, and features a mix of realist, consequentialist and idealist elements.

This approach equates the act of intelligence gathering and analysis to the use of force in war. Under this assumption, with war and intelligence becoming two facets of the use of force, Just War principles could be adopted for developing an ethical framework for intelligence. Accordingly, just as in war, principles of just cause, just intent, probability of success, proportionality, last resort, competent authority and discrimination should all be followed for intelligence to be considered just.

However, the problem with Just Intelligence approaches is that respecting their criteria does not necessarily make intelligence more just. As Phythian (2013) claims, actions that are blatantly in violations of human rights and international conventions – and that can be clearly morally questionable acts – may be perfectly permissible under a just intelligence framework.

First, in war, targets are either "black or white": they are either combatants or civilians. This is different in intelligence, where there is no real demarcation between actors involved in national security and ordinary people: there are, rather, various degrees of participation in the intelligence game.

Moreover, another criticism stems from the fact that just intelligence frameworks deprive the intelligence officer from his moral agency, placing it outside of his control. Just intelligence frameworks believe that moral decisions can be taken at a level higher than the individual, equating the role of the officer to the one of a soldier. These approaches *involve subjective judgments taken in specific national contexts* (Phythian, 2013). Who decides if the "cause" is "just" or not?

The issue is intrinsically linked to the conception of intelligence behind such approaches. We have seen that most of these approaches give intelligence agencies a specific role, which is essentially based on a misunderstanding of the role of the state on both domestic and international level. As Phytian (2013) argues, these frameworks over rely on a *Weberian conception of the state as being defined by its claim to the monopoly of legitimate violence with the idea of the "protecting state".*

Most importantly, wars are, as Phythian (2013) argues, an exceptional event. In exceptional circumstances, certain moral norms may exceptionally be suspended, hence the need for just war frameworks. Intelligence is, instead, a continuous process. It needs coherent and universal moral standards that can be considered acceptable in every moment, as the distinction between "peace" and "war" has no intelligence equivalent (Phythian, 2013). These considerations make clear that covert action and gathering cannot answer to the same ethical standards anymore. Covert action may perfectly fit the criteria for exceptionality that makes war legitimate

under just war framework. The same cannot be said for intelligence gathering, as it is an everyday activity that takes place even during peacetime.

If we want to steer away from realist conception of intelligence ethics, however, it is probably best to explore the possibility of circumscribing intelligence action within certain limits. To do so, however, we need to abandon some concepts and provide a redefinition of others: first of all, we need to define precisely what harm could be made to people by agencies, and in what measure it can be considered acceptable. Second, it is evident that the conception of national interest that has been adopted until now is restraining our analysis, and is in desperate need of a redefinition. Only in this way we will be able to achieve a universal framework for intelligence ethics that it is based contemporarily on individual agency, freedom and equality. This does not necessarily imply abandoning the whole just intelligence framework, but rather redefining and adapting it to our necessities by focusing on some specific elements.

Before going further, we must assume that there must be some limits to intelligence action. It would be unwise for agencies to conduct their everyday activities unrestrained, so it is obvious that some practical limits to their action must exist. In practice, these limits are mostly legal. It is important to remember, once again, that intelligence agencies are part of the government. As such, they are bound to operate under the rule of law.

Can exceptions to the law exist? As Giorgio Agamben (2003) argued, every constitution envisions clauses for a *state of exception*. What Agamben argues it that every political systems embeds in its constitution some kind of self-destruct mechanism that enables the same rights expressed in the constitution to be suspended or diminished, in the event of supposed national crisis. This means that, in case of emergencies, legal limits to intelligence are usually circumvented easily. The national interest apparently still takes priority over laws.

However, this mechanism is regarded as intrinsically dangerous. As we already argued, intelligence is a continuous process: therefore, it cannot operate in a continuous state of exception from the law. Exceptions can take place, but they have to be exceptions, literally. Intelligence needs clear and well-defined boundaries that

are always valid. And, still, the existence of exceptions does not make the acts of agencies made under a "state of exception" less morally questionable.

These considerations on legal boundaries, however, do not help us solve our problems. While morals and laws may overlap, it is important not to confuse legality with morality. Also, if a practice used for intelligence collection is unethical, making it legal does not eliminate the moral concern. This is a common mistake that many policy-makers have made in the past, and the actions of George W. Bush, who pushed for a redefinition of the crime of torture, believing that legalizing unethical practices like waterboarding would have made such practices legitimate, act as a constant reminder of that.

This suggests us that we need to move further away from identifying legal boundaries of intelligence action and start on reflecting on their moral boundaries. To define them, however, we need to ask ourselves first what harm could agencies do to individuals. In this way, we will be able to identify what agencies should refrain from doing on the basis on the way their actions harm other people.

If we want to identify what the moral limits of intelligence may be, asking ourselves what harm could be made to individuals because of abuses done by intelligence agencies is surely a decent starting point. This approach enables us to treat individuals, people, as the ultimate moral recipients of our framework.

How do we understand if an individual has been harmed or not? To do so, we need to identify a common set of values that satisfies two requirements: as Bellaby (2012) puts it, these values have to be vital to the well being of the individual and they have to be vulnerable to external influences. These values should be vital because they would be would be fundamental for enabling individuals to pursue their own goals and aspirations, and any restriction or damage done to them would cause harm regardless of its consequences (Bellaby 2012). They should also be vulnerable to external influences, as any damage done to these values should not come as a consequence of the actions of the individual, but from circumstances outside of his control.

Feinberg (1987) identifies a similar body of interests, and distinguishes between welfare interests, which are minimal, and ulterior interests that related to people's interests and goals. It is important to note that these interests go beyond human rights: those are the things that every free and equal individual needs to pursue his rational plan of life, human rights included.

We then would not go too far from reality if we accept Bellaby's (2012) claim that, in-between these vital interests, the ones who are more likely to be subject to restrictions due to intelligence gathering activities would be the *individuals' physical and mental integrity,* along with *their autonomy, liberty, sense of self-worth and privacy*. It follows that any intelligence action that impairs one of these "interests" in any way is therefore damaging other individuals, as it impairs their freedom. And it is clear that a moral obligation arises to prevent violation of these interests.

We finally meet our conundrum. How do we reconcile the need to protect these rights with the national interest? And, most importantly, can the national interest provide a sufficient motivation to circumvent these limits?

We need to rethink the concept of national interest as a moral construct, detached from the historical and societal contingencies that came to produce it. In direct contrast with Morgenthau's (1949) realism, we will claim that yes, there are supra-national moral principles concrete enough to give guidance to the political actions of individual nations.

We want to value autonomy and equality of opportunities above everything else. We then agree that all the vital interest and the institutions put in place to safeguard them ultimately serve the purpose of ensuring that everyone can benefit from autonomy and equal opportunities, and there are few reasons not to believe that people would not agree on their vital interests being protected, regardless of their citizenship. The national interest would then coincide with upholding and safeguarding these vital interests and protecting them from external threats. Therefore, as long as morals and laws concern these vital interests, concerns about ethics and legality are always in the national interest, and there are no reasons why these concerns should be overridden. Overriding them would be incoherent: why

would you let your intelligence agency violate these principles – abroad and domestically – if you want to value these principles above everything else? Also, we will argue that maintaining and preserving the institutions that are supposed to protect these vital interest is a vital interest in itself: put simply, the existence institutions that are unable or unwilling to ensure the protection of these interests can harm citizens directly, as the absence of these safeguards leaves them vulnerable to potential harm.

This conception of the national interest is clearly in contrast with the realist tradition, when Hans J. Morgenthau asserted in 1949 the primacy of the national interest over moral concerns: "*A nation should pour into the general principles of morality its own national conception of them, and then try to impose those moral principles, universal in form and national in content, upon the rest of mankind with fire and sword".*

Our reflections turn the realist position around: the national interest cannot provide a sufficient motivation to circumvent the moral – and legal – limits of intelligence, simply because these limits are there for the national interest. We are assuming that, in our societies, people would hold their rights and their freedom in their highest regards. What is the point of national security if it hinders these interests?

This means that intelligence agencies have a clear moral obligation not to violate these interests, because they are there to safeguard them. And, of course, this conception also implies a perspective shift on how the tasks of intelligence agencies are often portrayed. Intelligence and security are the means to an end, but security is not the end on itself, the ends are the people and their vital interests, since that is the only national interest.

Furthermore, we claim that, while the main objective of intelligence agencies is to protect their citizens' capacity to enjoy their vital interests, this has to be done with due respect to the vital interests of the citizens of other states. As a result of the hypothetical contract, intelligence agencies would have the moral obligation not to interfere with foreign citizens' vital interests. That is the turning point of our

argument: under the original position, people would agree that intelligence gathering methods conducted against them would be unacceptable should they hinder their vital interests. This is basically an application of the Golden Rule, in its negative form: *one should not treat others in ways that one would not like to be treated*. Why would an innocent citizen be subject to abuses from intelligence services, when he did not consent to be treated this way?

These reflections suggest us that some restrictions of these vital interests may still actually take place. There are probably people that, by consentingly participating in the world of national security, may *expect to be treated* in a certain way, even if they may not like it. There are probably still some rights and freedoms that can be restricted, as long as there are individuals that are freely deciding them to put them at stake.

Consent, here, is the keyword. And, as Pfaff & Tiel (2004) put it, not only consent is ultimately the manifestation of our freedom of choice and action, but it is also the fundamental moral criterion for establishing a line of conduct towards other individuals. When a gambler consents to gamble his money on a horse race, he knows that there would not be any injustice in losing his money should his horse lose the race, as long as the race is not rigged. But if I did not gamble any money, it would not be just for me to pay for something I did not consent to be part of.

Intelligence, using lt. Mattox's (2002) allegory, is much like a football game. Everyone who joins a football game can join it either as a player or as a spectator. Just as the football players tackle each other, actions such deception, blackmail and other acts that may compromise a person's vital interests are all allowed between intelligence agents. But just as football player cannot tackle a spectator, an agent cannot use his power against a citizen. It all comes down, again, to consent.

Consent in "taking part in the game" implies, first of all, that the person making this choice actually had the freedom to do so. Autonomy is safeguarded in this framework in two ways: first, because an individual is free to pursue his own goals as long as his vital interests are safeguarded and, second, because an individual is free to choose whether or not risk them by entering the "national security game". But

equality is also protected: people are not subjected to unequal treatment just because they detain specific information, but rather depending on how much the target has compromised himself by taking part in the intelligence world.

Consent, however, is just one element of the picture. While Pfaff focuses on consent as the sole determinant for distinguishing targets, we argue that shared expectations play an equivalent role in intelligence ethics. Only by knowing what to expect from other players and what other players could expect from her, an individual can truly and consensually decide whether to engage in the game or not. Shared expectations condition how people behave and they interact with each other.

Consent in taking part in the game, along with shared expectations, contributes to shaping social roles. Roles allow for a much better and comprehensive identification of targets. The intuition here is that there are different kinds of players in the intelligence game, each one playing a different role and each one being allowed different – if none – restrictions of vital interests based on their consent and shared expectations. The criterion for what is morally acceptable and what is not changes depending on the role of each player. While similar, this is a far cry from just war distinction between combatants and non-combatants. There are many more roles in intelligence and there is no size-fits-all way to approach to each actor.

Pfaff & Tiel (2004), list five different categories of targets, depending on "how much" the target is involved in the game and their level of consent. First, there is the ordinary citizen; second, we have the person possessing sensible information without being aware of its value; thirdly, there is the person in possession this information, aware of its value but unaware of being targeted; then, we have individuals in possession of information, aware of its value, aware of being targeted and willing to release the information; lastly, the fifth level is where the game changes, as here we have the recruited agent and the intelligence officer. Our conception of roles may comprise many more categories, but these ones just listed are a satisfactory abstraction.

In the first two cases, any kind of abuse or restriction of primary values directed directly towards these people, who are innocent in the sense that they did not agree

to the rules of espionage, is unethical and unjustifiable under any circumstances, even in the case of national emergency. In these cases intelligence can only make use of open sources or non-intrusive non-harmful methods of collection. The third case is the tricky one, as some minor abuse - like deception or blackmailing - may be acceptable, as long as the target involved willingly took this responsibility when acquiring the information. They would have agreed, through their free will, to be part of the game.

The fourth case causes no concerns, as the target is well disposed to release the information and no harm is being made to him or other innocent people. In the last case, much more is allowed. Since this target is an individual who freely choose to be fully part of the game, Pfaff et al (2004) argue that, in this case, he may be subject to deception, incitement, bribery, blackmail - even with manufactured evidence - and appropriation. Of course, even here, there are limits to what can be done. As Bellaby (2012) claims, *all other things being equal, some interests such as physical and mental integrity can take precedence over the other interests such as autonomy, liberty, self-worth or privacy*. Torture, for example, may still pose as an ethical limit to intelligence gathering. It would be interesting to ask ourselves whether a terrorist withholding vital information that could safe other people's lives could be tortured during interrogation under this framework. The answer is not easy, while it is true that the collective commitment to protect these rights and goods gets hindered simply by torturing another person, it is also true that the individual expected this kind of treatment if he were to be captured and that his actions would have threatened the lives of other people.

In these cases, criteria of proportionality (and here we can use some help from just intelligence) should then help officers decide which methods to employ. Differently from just intelligence approaches, cost-benefit evaluations should not drive this decision, but should be rather driven by how much of our collective commitment towards respecting and promoting human dignity are we eager to give up by harming another person in order to protect other people from harm. This suggests that even action against another officer, agent and any other legitimate targets has to respond to some specific criteria for it to be ethical. As mentioned, agencies hold a moral

obligation to limit the roughness of their methods to the strictly necessary, even against legitimate targets.

We now approach the end of our argument. Do our findings mean that ethical or legal concerns may be overridden in espionage? No, what we argued just means that the boundaries of what is ethical and what is not are different from time to time, because the rule of the game may be different. In no way, even because of a supposed national interest, an innocent citizen should be deprived of his vital interest. And, still, action should be as measured and as less harmful as possible even against legitimate targets. Going past those ethical boundaries would contradict the same national interest that those intelligence services are trying to protect.

One last remark: we have not gone into details. Under this model, some kind of non-coercive, non-harming intelligence gathering (better known as indiscriminate pre-emptive spying – IPS) could apparently still be permitted, but there is still no consensus on whether this kind of intelligence collection is something that violates vital interest or not. The problem with modern intelligence is that this kind of intelligence is seemingly getting more and more invasive both because of technological developments and for shifting perceptions of each one's sense of privacy. We will take a look at these concerns, and much more, in the next part of this study.

Part II: intelligence ethics in the digital age

Intelligence has not remained inert to technological development. Intelligence has mostly been receptive to the developments in big data analysis. These developments have enabled intelligence agencies to scale up their SIGINT practices significantly, coming in possession of potentially immense surveillance capabilities. State surveillance is just a facet of intelligence, or rather a consequence of it. Using Lyon's definition (2007), we can identify surveillance as *the monitoring of the behaviour, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them*. This notion is not

incompatible with the definition of intelligence we have previously given, according to Chuter's definition (2011): surveillance still requires information secretly acquired from an entity, which that entity does not want you to have.

What we call big data is a multi-layered process facilitated by technological developments in the field of ITCs, closely tied to the trend of hyper-connectivity that is characterizing the new millennium. This process has lead to a gargantuan increase in the amount of information produced by the network. What has also changed is the way this information is registered: it is not just the data that increased in quantity, but also the tools that are used to record it. This process is only bound to accelerate in the near future, as each aspect of people's lives may be converted into data, a process that has now been called "datification" (Cukier, 2013).

This digital footprint is not easily cancelled, but it is rather stored under the form of data into servers that could be located anywhere in the world. Once the data is stored, it can then be processed by algorithms and then handed to human beings for interpreting them. There are many people and organizations making use of big data, from researchers, advertisers to, obviously, intelligence officers. As we see, the word big data refers to this whole process of production, collection, and analysis, a process that mirrors the three categories of actors involved, as Zwitter (2014) lists them: big data generators, big data collectors, and big data utilizers.

Big data is important for intelligence because is transforming cyber-intelligence, a branch of SIGINT, both qualitatively and quantitatively. Agencies can now track the movements, calls, transactions, and pretty much any other action of their targets. But big data also allows for profiling much more than single individuals, enabling the monitoring of whole communities. Much more controversial, however, are the opportunities opened by indiscriminate pre-emptive targeting: big data analysis allows for performing preliminary intelligence gathering (in order to determine the "legitimate" targets) on pretty much everyone. Linked to this process is also the blurring of borders between domestic and foreign intelligence, where cyber-espionage has blended with cyber-law-enforcement. Big data allows for targeting foreigners and nationals indiscriminately, and this, in practice, has also been facilitated by unclear legislation on the field. If we link these developments with

other intelligence-related trends such as the rapid diffusion of drones and automated software, the decline of real-world HUMINT and the diffusion of privacy-by-design tools, we see that the ethical foundations of intelligence start to shake. These development lead us to question whether our previous considerations on intelligence ethics may still considered valid, as the impact of these practices on vital interests is unclear, while basic definition of consent and responsibility are definitely put into question due to a system of dispersed morality which characterizes the digital arena.

Controversy exploded on June 2014, when Edward Snowden, a National Security Agency contractor, and his confidant Glen Greenwalt released to the public, with the collaboration of international media outlets such as the Guardian and the Washington Post, a large amount of confidential data from the NSA. Most of this data was related to the so-called Verizon and PRISM affairs, and revealed massive surveillance programs conducted by the NSA and its Five Eyes partners[27] over the last years.

The publication of the Snowden archives showed that phone companies were sharing their consumer data with the NSA; that private conversations were data mined and monitored by the NSA with the collaboration of ITC giants such as Apple, Google, Facebook and Microsoft; that the United Kingdom Government Communication Headquarters were monitoring global communications and sharing the data collected with the NSA; and that geo-localization information and financial transactions were monitored too (Berendt et al, 2015).

These acts – especially the PRISM affair – placed a new kind of spying into the spotlight: indiscriminate pre-emptive spying. Accordingly, targets were spied *en masse* on the basis of no prior intelligence, so to select suspected individuals (Travaglione, 2016). As Wisnewski (2016) describes it: with PRISM everyone is being spied upon, but no one is really doing the spying. Government agencies like the NSA have access to private information, such as religious beliefs, political views, etc., but for the most part, this information goes untouched and unseen.

[27] The Five Eyes, a group of countries with a tradition of collaboration in intelligence, are: the UK, the US, Australia, Canada and New Zealand.

Could these acts be considered an invasion of privacy? Undoubtedly, the way this surveillance was carried out was unprecedented both in its nature and scope (Wisnewski, 2016), and this has led many to believe the institutions that were supposed to protect their rights and interests were actually actively violating them and turning their state into a surveillance state, with Foucault's version of the Panopticon being evoked quite often. In this modern Panopticon, technologies allow for an almost complete and invisible observation of society in which everyone can be watched without being allowed to know if they are.

While discriminate targeting practices[28] (due to the actions of the JTRIG) have not remained uncontroversial, recent developments in big data gathering and analysis, as we have seen, have given rise to a much more controversial practice: indiscriminate pre-emptive spying (IPS). Here, this practices allows for *spying indiscriminate targets en masse on the basis of no prior intelligence, in order to identify suspect individuals* (Travaglione, 2016). This is the kind of spying that characterized NSA's PRISM program. IPS targets are supposed to be innocent, and this is why this practice is ethically dubious. There is no argument of reasonable suspicion: IPS targets are not targeted because they have made themselves a threat for other people, as data mining is supposed to discover suspect behavioural patterns or suspect communication networks among *ex ante* unsuspected targets (Travaglione, 2016). The great majority of the people targeted are no players in the intelligence game.

Is NSA's invasion of privacy justifiable in terms of security? And, most of all, can it be considered harmful?

Under our framework, distinction between targets is paramount. Agencies have no right to indiscriminately harm citizens, no matter their nationality or where they are residing. However, if those acts cause no harm to citizens, we should see no reason to reject them. This may seem like the case for IPS: as Wisnewski (2016) reports, there is evidence that autonomy and privacy are mediated through belief. Accordingly, an individual may not see her autonomy impaired in any way and act inhibited, as long

[28] Discriminate reactive spying (DRS), as Travaglione (2016) defines it, is the practice of spying on specific individuals or groups on the basis of prior intelligence, in order to verify some specific suspicions or to accumulate more evidence.

she believes his privacy was not violated, no matter if she was constantly monitored and surveilled.

We could argue that IPS may be acceptable if really harmless but, in order for it to be so, there is one necessary condition to satisfy: it has to remain secret. If the mass surveillance system is discovered, as it happened with PRISM, serious harm to people's autonomy may be done, creating a Panopticon situation where people are restraining themselves because of the fear of being watched.

PRISM-style spying, however, cannot be considered to be entirely harmless, even if it remains secret. When agencies monitor citizens indiscriminately, they are still violating a vital interest (or primary good), a violation that could potentially cause harm if discovered. Privacy, a vital interest, is violated, and since it is an institution supposed to protect it that is violating it, damage is being done to the integrity of the whole institutional system. Harm is done to citizens indirectly since the integrity of the institutional system put in place to protect their vital interests is itself a vital interest for the community. The institutions risk becoming morally corrupt, because they are here to protect a common good such as privacy and are actively violating it, going against the national interest and harming its own community. These institutions are also supposed to share commitment towards respecting these interest everywhere, no matter the nationality of the targets: under the reciprocity clause, if you do not want another state to wiretap into you, you should not want your state to do the same to other citizens too.

But, most of all, this kind of spying creates knowledge asymmetries, actively creating inequalities even if the targets are unaware of it. PRISM-like system create a significant power imbalance within a society, as the watchers can know everything about their targets, while the watched cannot even know if they are being spied upon. This creates systemic inequalities that are, again, harmful in general and undesirable for the national interest, in the sense that this system privileges a form of knowledge available only to those with access to costly resources and technologies (Andrejevic, 2014), de-empowering anyone else and consequently damaging democratic institutions.

But let us put these considerations aside and suppose that no harm is being made whatsoever. As Travaglione (2016) argues, this is the condition of "perfect voyeurism": from a strictly consequentialist standpoint, undetected voyeurism could be considered not morally objectionable as it causes no harm to its victims. Therefore, intelligence agencies, when performing IPS, they should ensure it to remain *undiscovered, unpublicised and unexploited,* for it to be morally justifiable.

However, according to Travaglione (2016), there is another condition that must be satisfied, and this is the condition of necessity. Accordingly, the moral presumption against invading privacy should be defeated only when security, the good provided by IPS, offsets it. This means that IPS must be causally efficient, proportionate and there must be no other less costly alternative.

This being said, even if we accept that IPS is morally admissible only when these two conditions are satisfied, there is a problem that cannot be overcome. As Travaglione argues, there is a paradox between the perfect voyeurism and necessity conditions, as both can never be satisfied simultaneously. As he argues, for IPS to be causally efficient it must be exploited; it if is exploited, however, the possibility of IPS to be detected and publicized increases, compromising the perfect voyeurism condition. Moreover, for IPS to be perfectly voyeuristic, it cannot be exploited, but if IPS does not lead to any concrete usage, it cannot even be treated as necessary.

Exploitation may not necessarily entail publicity. But, as Travaglione argues, *the only way to keep IPS secret would be to thwart the process of free public information.* This, however, harms again the accountability of democratic institutions, as citizens are kept unaware of what their state is doing.

If, to this criticism, we add back the aforementioned issues of inequality and institutional integrity, we have enough motivations to argue that IPS is morally objectionable in many respects.

However, there is still one significant objection to our reasoning, coming precisely from the consent-based approach we adopted. As we know, IPS targeting would not possible without all the recent developments in big data; more specifically, without

people uploading their data online, the NSA would not have had any person to target. Could it then be that all these people, even if surveilled indiscriminately, are all legitimately targeted since they agreed to their information to be used in a certain way when using certain products and services?

It is not surprising, then, that someone may claim that users gave their *informed consent* for big data collectors to gather their data and use it in a certain way when they started using these products and services.

The reality, however, is that normal people have barely any say when it comes to how their information is treated. This is the main problem: the basis of consent is eroded because moral agency, as Zwitter (2014) argues, is precisely dispersed. We define moral agency as an ability based on three innate conditions[29]:

4- Causality: *An agent can be held responsible if the ethically relevant result is an outcome of its actions*
5- Knowledge: *An agent can be blamed for the result of its actions if it had (or should have had) knowledge of the consequences of its actions*
6- Choice: *An agent can be blamed for the result if it had the liberty to choose an alternative without greater harm for itself* (Zwitter, 2014)

Generally speaking, if one of these criteria is missing, the individual cannot be held fully responsible for his actions. Big data, however, challenges the concept of individual moral agency, making us question what free will and individualism can be found in a hyper-connected society. More precisely, it is debatable whether the *knowledge* and *choice* principles are satisfied.

It is undeniable that people rarely look at terms and conditions of use, and it follows that, if the users are not entirely aware of the consequences of their action, we cannot make them entirely accountable for these results and big data utilizers cannot use this information in a way that could harm them. There is, basically, a lack of *knowledge* that prevents them from fully exercising their moral agency. It could also be argued that, even when consent is informed, people do not expect or consent to

[29] Mind it: the term "agent" used in the following definitions is not to be interpreted in the intelligence connotation of the term

the government using this information (Wisnewski, 2016) and, despite the data being already public, no one really considers suddenly being the subject of research in Twitter or Facebook studies (Zwitter, 2014).

It is true, however, that we all should have looked at the terms and conditions of these services (even if pretty much nobody does it). However, even if people were fully informed about the way their information was going to be used, we can argue that users did not have much *choice* anyway. People use these products and services for a wide number of reasons: there are clear benefits for using these products, as there are clear disadvantages for not using them when everyone else is. By keeping them out of social media or other services, people miss out on social interaction and many other opportunities. For example, many may miss out on job opportunities coming from Linkedin, while others may also actually lose money by not having any Internet presence. This suggests us that the price to separate oneself from society may actually be too high, and that people do actually harm themselves by choosing not to "go digital". Some may be fully aware of the potential loss of privacy, but the lack of alternatives prevents these people from making an independent choice. As Tulloch (2016) puts is, the *entwining of the self and the social with digital technologies is irresistible*. There usually is no choice but *hyper-connectivity*.

Also, information may now be uploaded online even without the consent of the individual, even if no consent was given. Jonas (2015) reports at least two trends that are leading to bypassing choice and consent: first, the development of the Internet of Things (IoT), and second, acquaintances and friends inadvertently handing over the data of another person.

But it is not only the moral agency of big data generators that is impaired: recent developments in big data analysis and the decline of "real-world" HUMINT, however, have led to a process of dispersion of moral agency that has eroded the responsibility intelligence officers and agencies too, bringing the *problem of many hands* in intelligence. Where does the responsibility lie when personal data is gathered and privacy is breached? The problem is that, looking at the three conditions for moral agency (Causality, Knowledge and Choice), all the three actors involved in the big

data process – and, more concretely, in the PRISM controversy – can be found either deprived of these conditions or sharing the responsibility for many decisions.

Using Floridi's (2013) conception of *infraethics*, we argue that the *framework of implicit expectations, attitudes, and practices that can facilitate and promote morally good decisions and actions* has lost meaning in the digital arena. There are conflicting conceptions amongst actors of trust, respect, reliability, privacy, transparency, freedom of expression, openness (which Floridi all lists as moral enablers for infraethics), leading to contradicting expectations and morally bad outcomes. The only solution to this conundrum is reforming the system of infraethics by introducing new *moral enablers* (and enforcing pre-existing ones) so to reduce bad unintended consequences and spur a virtuous cycle amongst all actors, while defusing and removing all the *moral hinderers*.

Snowden's revelations have also brought attention to one final issue linked to individual moral agency. How should an officer behave if he knew that his agencies and his fellow officers were not respecting their obligations, and harming other people, how should they act? This is the same dilemma Snowden was faced with: should he have leaked these documents? He felt that NSA actions were violating fundamental rights and liberties, so he leaked them and yet, for exposing these illegitimate practices, he is now confined to Russia as twenty-one other countries refused his asylum-application (Travaglione, 2016).

Regardless of the direct consequences of Snowden's actions (be them negative or positive outcomes), it should be noted that, by leaking these practices, governments and agencies were put in a position where they could be held accountable for their actions. Indeed, not revealing these practices could be as much as harmful for democracy, whose integrity, we argued, is a vital interest in itself.

Is whistleblowing the only way, however? The options are limited: the officer can either *struggle from within the system* or quit and possibly publicly denounce this behaviour. Sometimes agencies provide ombudsmen for sorting these issues internally, but in other cases there is not much choice between staying silent or exposing the agency.

We have to think whistleblowing in a systemic perspective, as it may be fundamental for accountability. As we know, it is inevitable that the actions of intelligence agencies have to be kept secret. So who watches the watchmen? We can only rely on the officers themselves, and especially more morally minded ones: if the actions of an agency are crossing a line, a way to denounce these acts should be granted, first though some form of ombudsman, and second through some form of whistleblowing. The leaker should not be considered a traitor as long he denounces certain practices and not specific people (with the risk of endangering them).

The point is that if an agency is crossing a line and harming other people and their vital interests, it is the agency itself that is betraying its obligations towards its people. This is true even if it harms foreign citizens: under a veil of secrecy, we would not want an agency to harm foreign citizens as we do not know whether we will be on the receiving end of the abuse or not. Accepting whistleblowing may then have virtuous consequences on the system. Agencies, knowing that their officers could defect and denounce their bad practices, would probably restrain themselves from employing methods that could be considered unethical. Whistleblowing may then become a moral enabler for building a virtuous system of infraethics, using Floridi's (2013) terminology.
