Another Question Concerning Technology: The Ethical Implications of Homeland Defence and Security Technologies

John Jacob Kaag

INTRODUCTION

This essay begins to provide a unified moral reckoning with the way in which ideas concerning technological progress have altered the rules of military engagement and the implementation of homeland security. It will address both military technologies and technologies that secure the homeland, since the development and use of these technologies are vulnerable to the same ethical pitfalls. First, this essay employs Just War theory as a theoretical frame in which to situate the discussion and argues that the technology associated with precision guided munitions (PGM) only open the possibility of ethical discrimination and proportionality, but in no way insure that these possibilities will be actualized. Second, it begins to expose the relationship between the increasing popularity of PGM technology and the rhetoric that is used to describe contemporary military conflict. If precision weaponry is assumed to be inherently ethical, it may grant policymakers and strategists the chance to conflate the description of tactics with the prescription of normative judgements. Several case studies are employed to demonstrate this point. The second half of the paper asks if the technological progress that has come to define homeland security may lead to similar ethical difficulties in the fields of intelligence and law enforcement. It explores the way in which military technology and rhetoric might be redeployed in the domestic sphere.

The questions concerning PGM and homeland security technologies and their moral implications are also "questions concerning technology" – an interrogation of the moral and epistemic assumptions that seem to accompany and validate technical capabilities. It is a question that strikes at the heart of homeland security. When Martin Heidegger delivered "The Question Concerning Technology" to a Bavarian audience in 1955, he spoke at a pivotal historical moment in which technological advancements were beginning to be confused with political imperatives and the moral justifications of war. Today, we face a similar moment. The arms race of the Cold War may be over, but the danger that a blind faith in technological know-how poses to moral and rational sensibilities has never been as clear and present. In the end, this essay will suggest that technology itself neither answers nor ignores ethical questions; it is only the particular *use* of these technologies by practitioners that will either distract us from, or make us well attuned to, particular ethical questions concerning the rights and safety of the U.S. citizenry.

A JUST WAR ON TERROR?

The robust literature surrounding the issue of "just war" provides a helpful point of departure for a discussion of military technologies and their moral implications in homeland defence. This discussion will be employed later to

frame the discussion of homeland security. A brief review of Just War Theory may help to orient readers. Just War theory is usually addressed by way of two related constructs: *jus ad bellum* (justice in going to war) and *jus in bello* (justice at/in war).

Having a just cause is the first step in deciding to wage a just war. Any act of aggression is regarded as an unjust act and warrants a military response. In this context, a just cause is one that may be regarded as an act of immediate self-defence. Due to the narrowness of this definition, it is often broadened to take into account pre-emptive actions that are aimed to avoid future aggressive actions by another party. This expansion of self-defence to include pre-emptive military action will prove to be a slippery topic in our later discussion of "national security" and will be important in the designation of potential threats by homeland security officials. The second mandate of *jus ad bellum* states that a just war ought to be waged only when there is a reasonable chance of achieving the objectives of the mission. These issues are negotiated in the coming section, which asks if there is a relationship between technical capabilities that might ostensibly achieve objectives (capabilities that have been dramatically improved in the past decade) and the ability to designate potential threats to national security (an ability of judgement that remains difficult to hone). We must ask whether an increase in technical abilities might encourage a more liberal, and perhaps inaccurate, assessment of "threat" and national security. Before elaborating on this point, however, a bit needs to be said in regard to *jus in bello*.

Most scholars agree on at least two defining values associated with *jus in bello*: proportionality of means and precise discrimination. Proportionality generally refers to the degree to which military success is maximized through the use of minimal force. It is, at once, the demand to avoid *unnecessary* damage in any military strike. The definition of "just discrimination" is equally vague. Indeed, it flirts with a type of tautology, as seen in Dwight Roblyer's description: "discrimination means the separation of individuals into two categories: those liable to be *justly* attacked and those who should be immune to attack."[1] More generally, discrimination refers to the separation between the military and the civilian, between targets and non-targets.[2] The intent here is not to examine this distinction, but rather to notice the ways in which the advent of PGM seems to mask the ethical judgement that lies at the heart of this distinction. A similar examination will be conducted in reference to the "targeting" and monitoring of particular suspects who might threaten domestic security. First, let us take a careful look at the development of PGM in recent military engagement.

It might seem that the capabilities of PGM answer the two imperatives of Just War quite adequately. During Operation Enduring Freedom (7 October, 2001) and Operation Iraqi Freedom (19 March, 2003), the public saw an increasing number of photographs and film clips that seemed to reflect greater attention to these two Just War dicta. As of April, 2003, 80 percent of all bombs or missiles deployed by the U.S. Air Force in Operation Iraqi Freedom were guided by video camera, laser, or satellite targeting. In contrast, only 10 percent of all munitions employed in Operation Dessert Storm were so-called precision guided munitions.[3] Today, enemy targets appear to be targeted in highly populated areas with minimal collateral casualties; "smart bombs" enter windows and airshafts, seemingly detonating only where necessary. At

first glance, the "proof" of the munitions' effectiveness and surgical precision seems to respond to the call for military discrimination and proportionality.

First glances, however, can be deceptive. Precision guided munitions and remotely piloted vehicle (RPV) technology only opens the *possibility* of discrimination and military proportionality. Despite their "smartness," bombs *cannot* discriminate. Ultimately, the distinctions between enemy and innocent, and the choices of military cost-benefit analysis, fall to the human beings that drive the "targeting cycle" of a given military campaign.[4] This will be equally true in the case of homeland security officials in their attempt to identify suspects and conduct counterterrorism operations in the United States. This fact risks being obscured by the rhetoric of "progress" that surrounds advancement in military strike capabilities and in pinpoint surveillance technologies. As Michael Foley has noted, the "concept of progress has always suffered from a variety of logical and analytic problems which make it susceptible to ambiguity, disillusionment and abuse."[5] The relation between rhetorical ambiguity and technological progress will be brought out in the coming section, but a bit more needs to be said in relation to Foley's observation. The "abuse" that Foley cites arises when advancement in technology or know-how is not accompanied by corresponding efforts in ethics and political philosophy that might guide this advancement. In describing this abuse, Foley continues, "Progress in knowledge therefore resulted in proportionately less guidance over the direction to take it or which uses it should be served by it."[6] This tendency is reflected when progress in one venue, objective standards of casualty rate and destruction, are confused with normative standards of ethical justification.

In light of this situation, the decisions for military planners and homeland security officials have become more difficult and more morally charged. First, they must recognize the "abuse" hitherto described. Second, they must combat this abuse by redoubling their efforts to guide technical progress – instead of risking that technical progress might be allowed to guide moral sentiment. Finally, and to this end, they must recognize that the question is no longer one of sheer strike or surveillance capability, but rather one of dubious legitimacy. Granted, PGM helps avoid the catastrophic collateral damage that policy-makers faced during conventional or nuclear weapons escalation during the Cold War. However, as Dulles and Eisenhower pointed out in the early 1950s, the risk of Clausewitzian total war brought with it the practical constraints of self-preservation, often eliminating the role of moral choice in military planning.[7] Very simply, there is no real moral quandary when confronted with the choice between cold peace and thermonuclear conflagration. On the other hand, the quandary emerges with unprecedented force when the stakes of a particular case of military targeting are considerably lower and are often leveraged against individuals and groups that do not share the same sense of self-preservation. Similarly, contemporary forms of surveillance and counterterrorism, employed in domestic security measures, are now, with the help of modern technology, becoming so subtle and unobtrusive that they can easily be used without the knowledge of a given population. Indeed, these technologies are effective only to the extent that they remain undetected by a given community. To put this point another way, in the past, one did not have to agonize over the ethical implications of homeland security technologies for one of two reasons – either these technologies did not exist or, if they existed, they could not be employed nearly as subtly as they are today. When the

abuses of security technologies were more obvious, more transparent to the public, the choice to use or not to use them was more clear-cut for law enforcement agents. Now that digital and biometric devices have come to supplement our surveillance repertoire, the technologies do exist and can be used without a public's knowledge. This is the point where ethical debate concerning these issues ought to take root.

THE "PROGRESS" OF PGM AND SURVEILLANCE

Ironically, wars often become a viable, although questionably ethical, option when nation-states amass low-yield, precision-guided weaponry. A recent report issued by the Institute for International Strategic Studies suggests that PGM technology may lower the threshold that currently limits a state's military action.[8] In this case, military action may become the primary option, rather than the last resort, of foreign policy. This case seems to have emerged in recent U.S. actions in the Middle East and elsewhere. It seems not only possible, but also probable, that faith in the military modernization process allowed policy makers the chance to downplay alternative forms of soft power that might have been used in affecting change in particular territories. Soft power, as defined by Joseph Nye, is "co-optive" power – the ability to alter another's purposes by non-coercive means;[9] as E.H. Carr notes in *The Twenty Years' Crisis*, it is the "power over opinion."[10] The tendency to downplay this form of co-optive power in favor of the impressive coercive force of PGM is illustrated in the case of former Defence Secretary Donald Rumsfeld, a staunch advocate of the use of PGM, who is quoted by Nye as admitting that he didn't know what the term "soft power" meant.[11] Similarly, we might ask if the alternatives to technologically advanced, and subtly invasive, homeland security measures that jeopardize civil rights will be overlooked if policy makers become mesmerized by the capabilities of technology.

Turning to the issue of homeland defence, if we use the metric of unintended destructive force in order to evaluate the effectiveness and ethical standing of military strikes, it seems that PGM fits the bill quite nicely. However, while besieged populations may not be directly effected by the blast of a surgical air strike, the social, economic and humanitarian aftershocks of frequent PGM strikes may have lasting effects on the people of a surrounding area and the psychological landscape of the besieged population. As several commentators have highlighted, the societal upheaval *following* a military attack can take a real and deadly toll.[12] This is especially important if the intent of PGM use is to win military conflict, but also not to loose the "hearts and minds" of a given population.

Many policymakers claim that the risks of adjusting and lowering military thresholds are outweighed by the advantages of employing PGM in asymmetric conflicts in which particular objects and – more poignantly – particular individuals are liquidated with minimum "innocent losses." As the most recent conflict in Iraq has shown, such losses are still taken, albeit on a smaller scale. Human error still occurs. In the case of both homeland defence and homeland security, the ethical question of their implementation turns on the matter of *human* error. This point, however, is occasionally lost in the on-going attempt to increase technical capabilities. These capabilities are confused with ethical justification. For example, precision-guided munitions expanded the repertoire of strategic planners, including practices that were

hitherto excluded from the realm of Just War. Pre-emptive strike and the elimination of individuals with questionable military standing are becoming tools of standard U.S. military procedure. When Hellfire missiles can be launched from "standoff positions," targeting the cars of enemy military leaders, the art of war may quickly become the art of political assassination or summary execution.[13] It is true that these martial tools have a long history, but never have military planers and policymakers had to pay so *very little* to employ them. Precision guided munitions are used, at least in part, to avoid the loss of clandestine military ground forces and seem to answer the question of collateral damage. Both of these points may provide strategists and politicians *carte blanche* to target "potentially dangerous" individuals, to practice a form of selective targeting of questionable legality. This possibility needs to be confronted head on by policy makers and academics. The aforementioned practice is illegal under the International Covenant on Civil and Political Rights, the UN Principles on Effective Prevention and Investigation of the Extra-Legal, Arbitrary and Summary Executions, and Article 147 of the 4th Geneva Convention. We must weigh security against legal standing without allowing the story of technological progress to dominate the discussion of ethical norms.

John Yoo, who supports the successful targeting of the Hussein brothers in downtown Mosul, objects to this point, arguing that such surgical strike attacks should not be confused with illegitimate assassination:

> As Hugo Grotius, the father of international law, observed in 1646, 'It is permissible to kill an enemy.' Legitimate military targets include not just foot soldiers, but the command and control structure of an enemy's military, leading up to its commander in chief.[14]

Grotius may be right. It may be permissible to kill an "enemy." For Grotius, however, the question of specificity in military targeting could be answered rather easily. In *On the Law of War and Peace*, he adopts Livy's position, that "war is declared against the sovereign, and all within his jurisdiction."[15] This sovereign-centered approach to targeting, however, seems unhelpful and unrealistic as non-state actors emerge as the primary threat to international security.[16] Yoo surely recognizes this fact, yet fails to address a question that arises from these shifting security circumstances: In the age of asymmetric warfare and precision guided weaponry, who *exactly* is the "enemy?" Ironically, but not coincidently, the definition of "enemy" has become increasingly vague as the weaponry to deal with this ambiguous foe has become increasingly precise. This correlation is in no way arbitrary and is fraught with moral concerns.

Unfortunately, legal precedent is not extremely helpful in resolving the aforementioned situation. The rules of Hague Convention IV (1907) deal with counterinsurgency and revolutionary conflicts only in setting forth the conditions of belligerent status in Article 1. As William O'Brien notes, "Historically, the Hague Conventions were concerned with interstate, and the problems of unconventional war, even as a part of international conventional conflict, were not seriously addressed."[17] In light of the issues surrounding the use of unconventional force in World War II and Vietnam, it is surprising and disturbing that the Geneva Convention of 1949 and Geneva Protocol II of 1977 do not do a much better job of addressing the situation.

In his analysis of *jus in bello* in asymmetric engagement, David Rodin suggests that the increasing vagueness in military targeting is precisely the trend that must be counteracted if the principles of Just War are to be upheld. In so doing, he begins to revise the legal understanding of unconventional conflict and Just War Theory. He notes that as asymmetries arise, stronger military powers must assume a greater burden of proof in validating targeting techniques. For example,

> Western powers have historically considered dual use facilities to be legitimate military targets, but a more stringent interpretation of *jus in bello* (one that could be applied in the case of asymmetric conflict) would place all ambiguous targets and dual-use facilities that have important civilian functions off-limits for attack.[18]

Instead of emphasizing the stringency of Just War norms, an uncritical faith in precision technology, in *its* ability to discriminate, in *its* concern for the innocent, has occasionally allowed strategists and policymakers to employ vague rhetoric and fuzzy categories in defining enemy positions. A brief case study illuminates this point.

TECHNOLOGICAL KNOW-HOW AND THE AMBIGUOUS RHETORIC OF CONFLICT

Before the attacks of September 11, 2001, before the subsequent U.S. War on Terror, Gordon Graham made a prescient observation on the nature of enemy designation and targeting: "'Terrorism' and 'terrorist' are not descriptive words. They do not pick one sort of thing about which we might ask whether it is good or bad, but in themselves, serve to condemn whatever causes and methods the user of these words disapproves of."[19] This goes for the description of both international and domestic "terrorism." Today, these ambiguous, but powerful, watchwords dominate the discourse of U.S. international policy and have percolated into military targeting – targeting that is increasingly executed by PGM. Similarly, these words dominate the surveillance targeting of homeland security programs. This section will address the relation between the ambiguity of targeting language and the specificity of targeting execution. The literature on the rhetorical strategies President George W. Bush, Vice-President Cheney, and former Secretary Rumsfeld is well documented and underscores the possible moral shortcomings of these strategies.[20] Many of these accounts, however, overlook the way in which the development of highly specific weaponry and surveillance technologies have allowed – and indeed encouraged – the current administration to maintain its position in the War on Terror. This refers to the war at home and the war abroad. The use of this technology will not be unique to this administration and will continue to affect the deployment of particular rhetorical strategies.

The vital connection between the deployment of a technologically advanced military and the deployment of a general and ideologically-charged rhetoric became explicit in the fall of 2001. In the following statement, President Bush moves seamlessly from addressing military capacities to broad moral justification for implementing them:

> I have faith in our military. And we have got a job to do – just like the farmers and ranchers and business owners and factory workers have a job to do. My administration has a job to do, and we're going to do

> it. We will rid the world of the evil-doers. We will call together freedom loving people to fight terrorism…we've never seen this kind of evil before. But the evildoers have never seen the American people in action before, either - and they're about to find out.[21]

The slippage between capabilities and moral justification is enabled by the misguided belief that precise military action is inherently ethical. Is it appropriate for a "faith" in military-based surgical strike capabilities to grant policy makers confidence in their moral prerogative to "rid the world of evil-doers?"

Rumsfeld, a long-time proponent of PGM and RPV technology has also, not coincidently, been quick to provide broad-stroke, ethical justification for military strikes. At a 2003 press conference, the former secretary of defence stated:

> Our military capabilities are so devastating and precise that we can destroy an Iraqi tank under a bridge without damaging the bridge. We do not need to kill thousands of innocent Iraqis to remove Saddam Hussein from power. At least that's our belief. We believe we can destroy his institutions of power and oppression in an orderly manner.[22]

Rumsfeld opens with an assessment of technical military superiority that rests on the advancement of precision munitions. From these premises, however, he concludes that this superiority can be transferred to the moral realm, that technical precision can accurately "target" the *meaning* of "innocence," "oppression" and "order." This conflation between analytic description of capabilities and moral prescription is dangerous in its subtlety and stands as an ethical dilemma born from the development of PGM and other security technologies. For Rumsfeld, the "can" of security competencies implies an "ought" that is rarely examined in terms of stringent ethical guidelines. Rodin suggests that the tables ought to be turned when considering a nation's response to asymmetric threats:

> Pentagon and UK Ministry of Defence spokespeople never tire of telling us of the laser guided precision munitions and astonishing intelligence gathering capabilities at their disposal. Because Western powers have capabilities not possessed by weaker groups that enable them to achieve military ends with lower levels of collateral damage, it does not seem unreasonable to require them to do so.[23]

While I believe that Rodin's point is overstated and somewhat unrealistic, his general thrust – that U.S. policymakers and strategists must shoulder even greater responsibility in the targeting process – seems right. Instead of inspiring over-confidence, the revolution of military affairs (RMA) should give us ethical pause.

To this point, the discussion has focused on the moral difficulties that are raised in the refinement and the employment of PGM technologies. These difficulties are bound to be exploited by those individuals and groups who *do* seek to attack a highly mechanized military such as that of the United States. As a result, PGM targeting will only become more problematic. In light of this possibility, it seems wise to provide morally sound alternatives to the current coupling of fuzzy categories and precise surgical strike capabilities, alternatives that would allow strategists to avoid overstepping the bounds of international law. Steps are being made in this direction.

In Operation Enduring Freedom, the Department of Defence demanded that legal advisors be present at every stage of the targeting cycle to insure that commanders and strategists adhered to international law. U.S. Air Force legal reports indicate that military planners were, on the whole, "overly cautious" when faced with the responsibility of initiating strikes, a responsibility made more acute by the use of PGM. These reports also indicate that such hesitancy may, in fact, prolong human suffering by extending the duration of military operations.[24] This assessment, however, stands against most evaluations of PGM targeting. While the presence of legal advisors in the targeting process is sure to alleviate some of the moral concerns surrounding PGM, it may provide policy-makers a false sense of ethical legitimacy.

THE MORAL SHOCKWAVE OF TECHNICAL CAPABILITIES

It is worth noting that all military targeting, and particularly PGM targeting, begins with precise intelligence gathering and the methods employed therein. Legal expertise must be brought to bear on these methods as well and should dovetail with a study of precision guided munitions. "Painting" and destroying specific enemy targets with laser-guided precision often depends on the reliability of intelligence garnered from the interrogation and coercion of enemy prisoners. The demands of PGM targeting, the need to specify an enemy's exact position and character, may place undue burden on interrogators who feel responsible for providing this information.

This is not to suggest that PGM technology is a direct cause of informant/prisoner abuse; it surely is not. It is possible, however, that the effort to implement effective PGM strikes may indirectly encourage moral crises in other areas of the armed forces. If we give priority to the accurate targeting of enemy combatants, which seems like a reasonable priority, we may have to go to extreme measures to glean proper intelligence. The pursuit of one moral outcome (discrimination in the targeting cycle) may force us to give up others (proper interrogation procedures and not detaining suspects without legal mandate). This is not to set up unrealistic or impossible standards for the homeland security or homeland defense official, it is only to underscore the relatedness of various ethical issues. This is the moral "shockwave" of the revolution of military affairs and the ever-advancing forms of security technology.

A final shockwave of security and defence technologies needs to be addressed, for it will only continue to reverberate as technological know-how drives the trends of the revolution in military affairs and homeland security. Commentators often discuss the way in which surgical strike technology helps strategists avoid civilian collateral damage. Similarly, pinpoint domestic intelligence is lauded for avoiding the "blanket approach" to surveillance that might eviscerate the civil rights of an entire population. Additionally, the use of PGM and RPV arguably reduces the risks to military personnel in many engagements. Similarly, anti-terrorist technologies employed in the "homeland" are meant to protect security agents in the field. It is fair to celebrate both of these points – and celebrate them earnestly. This being said, it seems wise to address the way in which limiting troop losses might affect the duration and execution of wars. Similarly, it seems wise to address the way in which protecting field agents might affect the objectives and duration of a domestic security program. Would a prolonged War on Terror be possible

without the technological know-how of the 21st century? How does technological capability, rather than sustained and democratic discourse, determine the shape and duration of this war? While a detailed study is beyond the scope of this essay, a few questions are warranted. First, what is the relation between troop losses and public support of a particular conflict? Do constant, yet low-frequency, losses – the kind of losses that are suffered in guerrilla warfare in which PGM are currently used – insulate strategists and policymakers from a democratic outcry that might affect the course of a conflict? To what extent is this development beneficial? While surgical strike capabilities allow military and security planners to do their jobs effectively, is there a type of technological-institutional inertia that may encourage an uncritical acceptance of current tactics? Finally, what are the fiscal and budgetary considerations of PGM and surveillance technologies? Will technological progress in security programs, developed to protect liberal ideals, outstrip a nation's ability to provide liberal institutions to its citizens? In all of these questions, it is necessary to remember that it is not the advancement of technology that is question begging, but rather the purposeful use of this technology by moral agents that must be re-interrogated.

In 1947, at the dawning of the nuclear age, President Truman set forth a goal that remains elusive:

> We must catch up morally and internationally with the machine age. We must catch up with it, and we must catch up with it in such a way as to create peace in the world, or it will destroy us and everybody else. And that we don't dare to contemplate.[25]

In 2004, at the dawning of another military era, the "machine age" continues to outstrip our moral practices and ethical sensitivities. While the use of precision-guided munitions *seems* to satisfy the longstanding mandates of Just War, in fact, it only complicates the moral standing of armed conflict. In short, precision-guided munitions create as many ethical dilemmas as they solve. Policy-makers and military strategists may forgo the target of morality at an ironic moment, at a moment when precision weaponry *seems* to grant them the clearest shot.

HOMELAND SECURITY TECHNOLOGIES: WHEN "NEW" MIGHT NOT ALWAYS BE BETTER

How does the discussion of the ethical ramifications of PGM bear on the issue of homeland security? This question seems important to the extent that the technologies employed abroad in the War on Terror have also defined the rhetoric and practice of domestic security. As the National Research Council noted in a 2003 report on homeland security technologies, "The science and technology required by the Army for Homeland Security need not be unique. The science and technology work already being done for the Objective Force (HD) could provide much of the technology needed for Homeland Security"[26] Before proceeding, it is necessary to note that this discussion addresses homeland security only in its capacity to implement counter-terrorism measures. In short, it assumes the "strict constructionist" perspective that Christopher Bellavita describes as a position that echoes the traditional understanding of homeland security in the *National Strategy*.[27]

That being said, this analysis of homeland security technologies will address three interrelated issues and may provide a helpful model for future

investigation. First it will briefly address establishment of a specialized branch of DHS that focuses on technology research and development. A comment on the growth of this branch, coupled with several observations concerning the 2001 U.S. Patriot Act, will provide the rationale for examining both the technological advancements in the Revolution in Military Affairs and homeland security. Second, the discussion will examine the SAFETY Act of 2002 that was established to encourage research and development in "anti-terrorist technologies." Third, it will evaluate the potential synergy between surveillance and biometric technologies in the project of homeland security. All of these evaluations resonate closely with the earlier discussion of PGM to the extent that impressive technological capabilities may continue to be conflated with our ability to make normative judgements concerning innocence, guilt, and threat.

So where does the technology of homeland security come from? Many people would have trouble answering this question – perhaps even a few people who work in the bureaucratic monster of DHS. The answer to this question is complicated, but a good place to start is the Science and Technology Directorate of DHS. The directorate is lauded as one of the great success stories of the War on Terror. It is also a story that is often not told to the public and the details of which are often omitted. The anonymity of the directorate's scientists and the secrecy of its projects are necessary safeguards in order to maintain the effectiveness of security technology employment, but have the unintended consequences of fuelling Orwellian suspicions concerning technology and precluding open discussion concerning the ethical implications of the use of these technologies. The directorate was established in the winter of 2003 and was modelled loosely after the Pentagon's Defence Advanced Research Project Agency (DARPA) and the technology directorate at the CIA. Many members of the DHS directorate were trained in one of these two organizations. DARPA serves as the technological dynamo of the armed forces, providing soldiers in the field with the latest military tools. The technology directorate of the CIA is responsible for supporting field officers and intelligence analysts with technologically advanced means of counterterrorism and intelligence gathering. Here, it begins to make more sense why a discussion of the ethics of war might serve as an appropriate preface to the ethics of domestic security technology. The ethical blind spots in one arena of strategy may be imported into DHS policies. There are also powerful resonances between the rhetoric of war and the rhetoric of protecting the homeland by way of technological innovation that might give us pause.

In 2001, John Ashcroft described the two inter-related principles of the PATRIOT Act, stating that the first was "the airtight surveillance of terrorists" and the second was to increase the speed in "tracking down and intercepting terrorists." After employing the loose term of "terrorists" to identify threats to national security, Ashcroft gets to the very particular means of achieving this goal. His comment bears directly on the discussion of the ethical risks implicit in employing security technologies.

> Law enforcement officials will begin to employ new tools that will ease administrative burdens and delays in apprehending terrorists…Agents will be directed to take advantage of new, technologically neutral standards for intelligence gathering. [28]

Several points deserve to be underscored in this passage. First, it seems reasonable to expect that many of the "new tools" to which Ashcroft refers have their roots in *techne*, in the instruments (both physical and legal) that law enforcement officials can employ. "New" is not necessarily better, or more ethical. A long and sincere discussion is warranted in order to address the relationship between these new tools, oftentimes defined by their impressive technical capabilities, and the "administrative burdens" that Ashcroft sought to avoid. The term "administration" refers to a thoughtful human process that is shot through with normative claims and assumptions. Administration refers to a process of human judgment that is burdened with responsibility. Administration can never be substituted or "unburdened" by the mere use of new tools. Tools should be used, but must be used in the *right* way.

Second, it ought to be noted that the delay in apprehending criminals, a delay that Ashcroft wanted to avoid, has never simply been a matter of raw capability. It is equally a matter of judgement and due process. This fact needs to be considered carefully; as capabilities increase, it cannot be the case that due process and responsibility are abandoned in pursuing the siren calls of technological progress and security.

The appeal of technology need not be siren call – but it often is. This danger lurks in the background as Ashcroft reflects on his belief in "new, technologically neutral standards" of security implementation. The belief in the neutrality and objectivity of technology leads us away from meaningful discussions and debates concerning the ethicality of technology's use. It encourages us to forget that progress in the technical realm does not necessarily translate into the advancement of ethics or justice. The use of technology is never neutral. The creation of technology is never neutral. The ends of technology are never neutral. They are always part and parcel of the interests of individuals and groups that should be discussed, and in many cases, hotly debated. Additionally, Ashcroft's elision of "neutral standards" and technology seems more at home in the Scottish Enlightenment of the 1700s than in the political mindset of the United States in the 21st century. Standards are, almost by definition, *not* neutral. A standard is always a standard in reference to some point of view or to some agreed upon benchmark. This situation is question begging: If one forgets that standards are *human* measurements rather than unalterable technological products, does this effectively overlook the debate that might alter and revise these standards? This question emerges in the rhetoric of homeland security, but also in the legislation surrounding the development of new security technologies.

The Support Anti-terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 provides legal liability protection to the providers of qualified anti-terrorist technology. In his Congressional testimony in 2006, Jay Cohen describes SAFETY:

> These (liability) protections apply to companies when the worst happens – an act of terrorism. The SAFETY Act is intended to ensure that the threat of liability does not deter potential sellers or manufactures of anti-terrorism technologies from creating or providing products and services that could save lives.[29]

It is worth noting that Cohen's testimony was given four years after the SAFETY Act was accepted by DHS. Indeed, SAFETY did not receive a hearing

in either chamber of the legislature and was inserted into the Homeland Security Bill late in the legislative process when it was observed that the indemnification processes considered earlier would not suffice. The implementation of SAFETY is of concern for at least three reasons that coincide with the earlier discussion of PGM technologies.

First, the "anti-terrorist technologies" under the SAFETY act include information security systems, biometric devices, surveillance networks and perimeter intrusion detection devices. Biometric technologies potentially link the legal identities of visitors and U.S. citizens with their physical characteristics. The technical specificity and cost effectiveness of these products have dramatically increased in recent years. For example, surveillance technologies have become more efficient through the use of GPS and have become smaller, and hence more easily concealed. While this fact makes them more "effective," they potentially jeopardize some of the civil liberties that U.S. citizens have long enjoyed under the Fourth Amendment. These "products" also include the services that may support anti-terrorist technologies, services that might not be regulated by pre-existing guidelines.

Second, the technical specificity of these products has come hand-in-hand with an ambiguity in the language that is used to explain and justify these technologies. The SAFETY Act itself reflects this ambiguity in the sense that it is unclear whether the act provides "safety" to U.S. citizens or to sellers and vendors of anti-terrorist technologies who wish to be shielded from liability litigation. Cohen suggests that this act is necessary since it "saves lives," but he avoids addressing the costs of SAFETY on the lives and liberties of visitors and citizens. These costs might begin to be highlighted in a discussion of the way in which SAFETY could transform the common law doctrine of "government contractor defence" which hitherto limited the liability of sellers of contracted technologies to the U.S. government. Under this law, the government issued the specifications for the product and the manufacturer met these specifications with full disclosure. SAFETY, as written in 2002, begins to do away with this procedure. Under SAFETY, companies submit the specifications of their products and, if approved, earn a rebuttable presumption in future liability cases that can be overcome only by proof that the company acted fraudulently in the submission of these specifications. One might ask, in this case, who exactly is liable if the employment of "anti-terrorist" technologies does result in harm to the lives and liberties of U.S. citizens?

It appears that DHS might be willing to limit citizens' ability to present grievances in an attempt to curtail excessive tort litigation in the instance of anti-terrorist technologies. Recent developments in the SAFETY Final Rule (2006) indicate that it might also be willing to accelerate the testing and regulation cycles of these technologies.[30] When considered in tandem, these two comments ought to give us pause – if not a cause for genuine alarm. Is the loosening of tort litigation and the accelerating of product testing a viable long-term solution for the maintenance of homeland security?

To this point, this essay has not addressed specific technologies, but only discussed the ways of thinking and talking about their use. It has addressed the ethical blind spots that might characterize the use of security technologies without describing any specific homeland security measures. Two such measures will be addressed in conclusion: thermal resonance imagining and the Internet surveillance programs, Carnivore and Magic Lantern.[31]

The U.S. military, in night reconnaissance, targeting, and combat in obscure conditions, has used thermal imaging for many decades. This technology allows soldiers in the field to literally see through walls by detecting the thermal resonance of potential enemy combatants. Similar technologies are used in missile guidance systems that employ heat-seeking devices. This technology is beginning to "come home" in new ways, to be redeployed on the domestic front in the War on Terror. Implementation is in its early stages, but the implications of this technology should be confronted now. Thermal imaging can allow field officers to see a suspect hiding in the dark; it has recently been suggested that the same imaging can allow officers to see inside a suspect's head.[32]

When a person is upset, anxious or aroused, blood rushes to the face and particularly the eyes. This physiological effect can be detected on a thermal image. The eyes "light up" on the image. This technology has been developed in interrogation scenarios and now supports the most innovative lie-detection devices. Thermal imaging technology, however, is beginning to make its way out of the interrogation room and into U.S. customs, at the major points of entry to the United States. It is used to screen individuals who might attempt to enter the country with false documentation, assuming that these individuals will be more agitated than their fellow passengers. This practice may prove ethically problematic in the coming years. After our discussion of precision guided munitions, it goes almost without saying that in the case of detecting physiological effects, thermal resonance imaging can neither help officials judge the motives of a person nor determine the causes of a subject's anxiety. Indeed, these devices are not very accurate in determining the difference between anxiety and general arousal.

The members of the Israeli intelligence service and law enforcement agencies have become quite adept at detecting lies in potential terrorists. They did not achieve success by way of thermal imaging, but through a careful study of, and prolonged exposure to, the suspect's behaviour. Officials engage in extended conversations with subjects and then *make a judgement* concerning the truth or falsity of the subject's story.[33] This naturalized approach to lie-detection is an art form that is time-intensive and takes into account semantic, emotional, syntactical, and bodily cues. It is a holistic approach to lie-detection that cannot be approximated by an analysis of the thermal image of a subject's face. Thermal imaging seems to be a good first line of defence, but the discussion of PGM indicates that there may be a tendency to become mesmerized by the technological capabilities of these devices and allow them to take the place of human judgement subject to ethical evaluations. In short, we run the risk of developing a false confidence in this sort of technology. With this confidence may come a kind of complacency in our ability to make judgements – both ethical and practical.

The discrete character of thermal imaging cameras will eventually allow this sort of screening to be accomplished without disrupting the subjects of the investigation. This is a beneficial development, but it also raises questions concerning the legality and ethicality of these types of monitoring devices: are these "mental searches" ethically viable alternatives if subjects do not submit to them? Will these approaches be used more frequently as their subtlety and discreteness increases? Is this direct correlation a cause for concern?

A similar set of question might be posed in reference to what Etzioni calls "public protective technologies" that have recently been developed to regulate

and screen the uses of the Internet.[34] In 2000, the FBI unveiled Carnivore, a computer program designed to sift through the stream of many millions of messages between individuals who may, or may not, be engaging in criminal activity. As Etzioni notes, many ISPs do this sifting themselves and pass along information to authorities when a warrant is obtained. If the ISP is not able to do this, however, Carnivore is.[35] Carnivore's filters are set in accordance with legal court orders, but these filters are necessarily general and include the communications of many other users than just the suspects. Despite Carnivore's breadth (the ability to filter millions of messages in a short period of time), it lacks depth (the ability to break encrypted code, the likes of which are used in many electronic correspondences).[36] This is where Magic Lantern comes in. As compared to "keystroke capture" devices such as the Key Logger System (KLS), which have to be manually (and covertly) installed on a suspect's computer, this device is considerably less invasive. Like the Key Logger System, it does not decrypt particular emails, but grants authorities access to a suspect's password. Instead of placing additional hardware on a subject's computer, as does KLS, Magic Lantern allows the FBI to place software on a computer by way of a virus-like program. Just like a virus, Magic Lantern can be imported into a suspect's computer by way of the Internet. The American Civil Liberties Union compares the use of both of these devices to agents ripping "open each and every mail bag and search for one person's letters" and tapping an entire phone system instead of targeting just one caller.[37]

CONCLUSION

The advent of highly specific technologies, often employed for the screening of people, their communications with others, and patterns in their behaviour, leads us back to the issue of "targeting" which rested at the centre of the debate concerning PGM. While military targeting in homeland defence departs in significant respects from the "targeting" or identification of particular individuals who jeopardize homeland security, certain similarities warrant discussion as Homeland Security and the SAFETY Act take shape in the coming years. As suggested in the sections focusing on precision-guided munitions, as the political, material, and economic costs of employing technologies declines, the prevalence and frequency of their use tends to increase regardless of the ethical implications. Indeed, the sheer utility and effectiveness of security technologies may *seem* to make discussions concerning their ethical use almost superfluous. Even in light of judicial oversight and warrant requirements, analytic descriptions of capabilities are often conflated with normative prescriptions or designations. This rationale may prevail in homeland security if the reason to "target" citizens and visitors is reduced to the fact that it is easy to do so with the help of affordable precision technologies. Technical capabilities appear ethical in their ease of use, their precision, and their cost-effectiveness. Such appearances, however, should not deceive us. The first step in initiating an ethical discussion concerning security technologies is to recognize that there *are* ethical decisions to make, that technology itself cannot answer these questions, and that these questions deepen and multiply as technological capabilities increase.

In outlining the PATRIOT Act, the attorney general stated that he planned to "shine the light of justice" on wrongdoers. This essay has suggested that the light to which Ashcroft refers does not necessarily emanate from "justice," but from highly specific technologies that may be easily masked in the rhetoric of justice. When Martin Heidegger gave his lecture on "The Question Concerning Technology" in 1955, his main concern was the way in which technological know-how may come to dominate the entire field of human knowledge and judgement. He suggests that technology is a "way of revealing," a way of ordering things to "stand by," a way of putting things and people "on call for a further ordering."[38] This suggestion strikes at the heart of Ashcroft's understanding of shining the light of justice on potential terrorists. Many security technologies, used in either just or unjust projects, place people "on call for a further ordering" and demand that they stand by or stand trial. The risk involved in the use of modern technology in homeland security is that it may overshadow other forms of reflective judgement, and that its impressive capabilities may distract us from the sobering discussion of ethics. In a commentary on Heidegger's lecture, David Krell states that the "question concerning technology confronts the supreme danger, which is that this one way of revealing beings may overwhelm man and beings and all other possible ways of revealing."[39] Krell and Heidegger are onto something here. There is a supreme danger that technological ways of revealing will become synonymous with "shining the light of justice" on potential enemies. There is the danger of confusing technical capabilities and just norms.

At this point it seem wise to return to the ethical balancing act that Ashcroft outlined in his comment after September 11, 2001: "We always have to be careful that the rights which America stands for are protected, but we also have to understand that in order for those rights to be enjoyed, they have to be protected."[40] Security technologies, however, *do not* help us negotiate the dual commitment of rights and protection. Indeed, the fact that technological "progress" risks becoming equated to ethical progress will make moral questions harder to frame and harder to answer. We must hone our ethical senses and sensibilities in order to keep up with the technical know-how that broadens the field of possible strategic choices.

John Kaag is currently a 2007-2008 visiting scholar at the American Academy of Arts and Sciences and a research associate at the Humanities Center at Harvard University. His work has dealt with social-political thought in the early American philosophical tradition and has been featured in the Journal of Speculative Philosophy *and the* Transactions *of the Charles S. Peirce Society. He received his PhD at the University of Oregon in the summer of 2007 and an MPhil in International Relations from Cambridge University (UK) in 2004. Professor Kaag may be contacted at jkaag@fas.harvard.edu.*

---

[1] Dwight Roblyer, *Beyond Precision: Issues of Morality and Decision Making in Minimizing Collateral Casualties* (Urbana-Champaign: University of Illinois Press, 2003), 4.

[2] James Johnson, *Morality and Contemporary Warfare* (New Haven: Yale University, 1999), 37.

[3] "Today's Bombs Smarter, Cheaper." *CBS News*. March 25, 2003.

[4] Colm McKeogh, *Innocent Civilians: The Morality of Killing in War* (New York: Palgrave, 2002), 54.

[5] Michael Foley, *American Credo: The Place of Ideas in American Politics* (Oxford: Oxford University Press, 2007) 87.

[6] Ibid., 27.

[7] John L. Gaddis, *Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy* (New York: Oxford University Press, 1982), 135.

[8] *Strategic Survey 2003/4: An Evaluation and Forecast of World Affairs* (London: Oxford University Press, 2004), 23.

[9] Joseph Nye, *Soft Power: The Means to Success in World Politics* (New York: Public Affairs, 2004), 8.

[10] E.H. Carr, *The Twenty Years' Crisis* (New York: McMillan, 1964), 34.

[11] Joseph Nye, "The Decline of America's Soft Power," *Foreign Affairs* (May 2004): 51.

[12] Eric Hooglund, "The Other Face of War," *Middle East Report* 171 (Aug. 1991): 3-12.

[13] John Yoo, "Legally Dead," *The Weekly Standard,* August 11, 2003, A7. In the winter of 2002, the CIA reportedly launched a Hellfire missile that killed al Qaeda leader Qaed Salim Senyan al-Harthi while he drove a car in Yemen. .

[14] Ibid.

[15] Hugo Grotius, *On the Law of War and Peace*, trans. Walter Abrams (New York: Kessinger Publishing, 2004), 98.

[16] Pojman notes that "Critics (of Just War theory) contend that it is a holdover from the confined medieval battlefield, with knights on horses voluntarily engaging the enemy in the name of the king…it has little to do with the modern world." In Louis Pojman, *Global Political Philosophy* (Boston: McGraw Hill, 2003), 224.

[17] William O'Brien, *The Conduct of Just and Limited War* (New York: Praeger Publishing, 1981), 175.

[18] David Rodin, "The Ethics of Asymmetric War," *The Ethics of War: Shared Problems in Different Traditions*, ed. R. Sorabji and D. Rodin (Ashgate: Oxford, 2006), 161.

[19] Gordon Graham, *Ethics and International Relations* (Cambridge: Blackwell Publishing, 1997), 116.

[20] For example, see George Lakoff. *Whose Freedom: The Battle over America's Most Important Idea.* (New York: Farrar Straus and Giroux, 2006); Stefan Halper.and Jonathan Clarke. *The Silence of the Rational Center.* (Cambridge: Cambridge University Press, 2007); Noam Chomsky. *Hegemony or Survival: America's Quest for Global Dominance.* (New York: Metropolitan Press, 2003).

[21] "Remarks by the President Upon Arrival – South Lawn" Press Briefing. September 16, 2001, http://www.whitehouse.gov/news/releases/2001/09/20010916-2.html.

[22] "Department of Defence News Briefing – Secretary Rumsfeld and General Meyers," March 28, 2003, http://www.defenselink.mil/transcripts/2003/t03282003_t0328sd.html.

[23] David Rodin, "The Ethics of Asymmetric War," 163.

[24] *Air Force Operations and the Law: A Guide for Air and Space Forces* (Washington D.C.: Air Force Judge Advocate General's Department, 2002), 298.

[25] "Remarks at a Meeting with the American Society of Newspaper Editors," April 17, 1947, www.trumanlibrary.org.

[26] National Research Council, *Science and Technology for Army Homeland Security: Report 1* (Washington, DC: National Academies Press, 2003), 22.

[27] Christopher Bellavita, "Changing Homeland Security: What Homeland Security Leaders Should be Talking About," *Homeland Security Affairs* 2, no. 2 (2006): 6.

[28] Cited in Howard Ball, *The USA Patriot Act* (Santa Barbara: ABC-CLIO, 2004), 68.

[29] Jay Cohen, "Congressional Testimony," *Congressional Daily Digest*, September 13, 2006.

[30] The Final Rule stipulates that the testing cycle will be reduced from 150 days to 120 days in order to expedite production. See SAFETY Final Rule (January 2006).

[31] For a detailed analysis of these technologies see Emitai Etzioni, *How Patriotic is the Patriot Act?* (New York: Routledge, 2004), 27-77 and Matthew Brezezinski, *Fortress America: On the Front Lines of Homeland Security – An Inside Look At The Coming Surveillance State* (New York: Bantam, 2004), 193.

[32] Ioannis Pavlidis. "Lie Detection Using Thermal Imaging." in *Thermosense*. Vol 26. (Washington SPIE Press, 2004), 270-279.

[33] Once again, the difference between technical output (the "lighting up" of an image) and human judgement should not be confused.

[34] Etzioni, *How Patriotic is the Patriot Act?* 60.

[35] Ibid., 61.

[36] United States Senate, *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Committee on the Judiciary,* 106th Congress 3 (2000).

[37] "Urge Congress to Stop the FBI's Use of Privacy Invading Software," 2001, http://www.aclu.org/action/carnivore107.

[38] Martin Heidegger, *Basic Writings: Revised and Expanded Edition,* ed. David Krell (San Francisco: Harper Collins, 1993), 322.

[39] Ibid., 309.

[40] Cited in CSIS Briefing, "Strengthening Law Enforcement Capabilities to Combat Terrorism," October 2003.