Les Marguerites Fleuriront ce Soir *by Jeffrey W. Bass, 2006. During the Second World War, Virginia Hall from Baltimore, Maryland conducted espionage in France for Britain's Special Operations Executive (SOE) and later for America's Office of Strategic Services (OSS). For her efforts, she received the Distinguished Service Cross, the only one awarded to a civilian woman in the war. She later served the CIA. Source: Central Intelligence Agency, via Flickr.*

JUST INTELLIGENCE, JUST SURVEILLANCE, & THE LEAST INTRUSIVE STANDARD

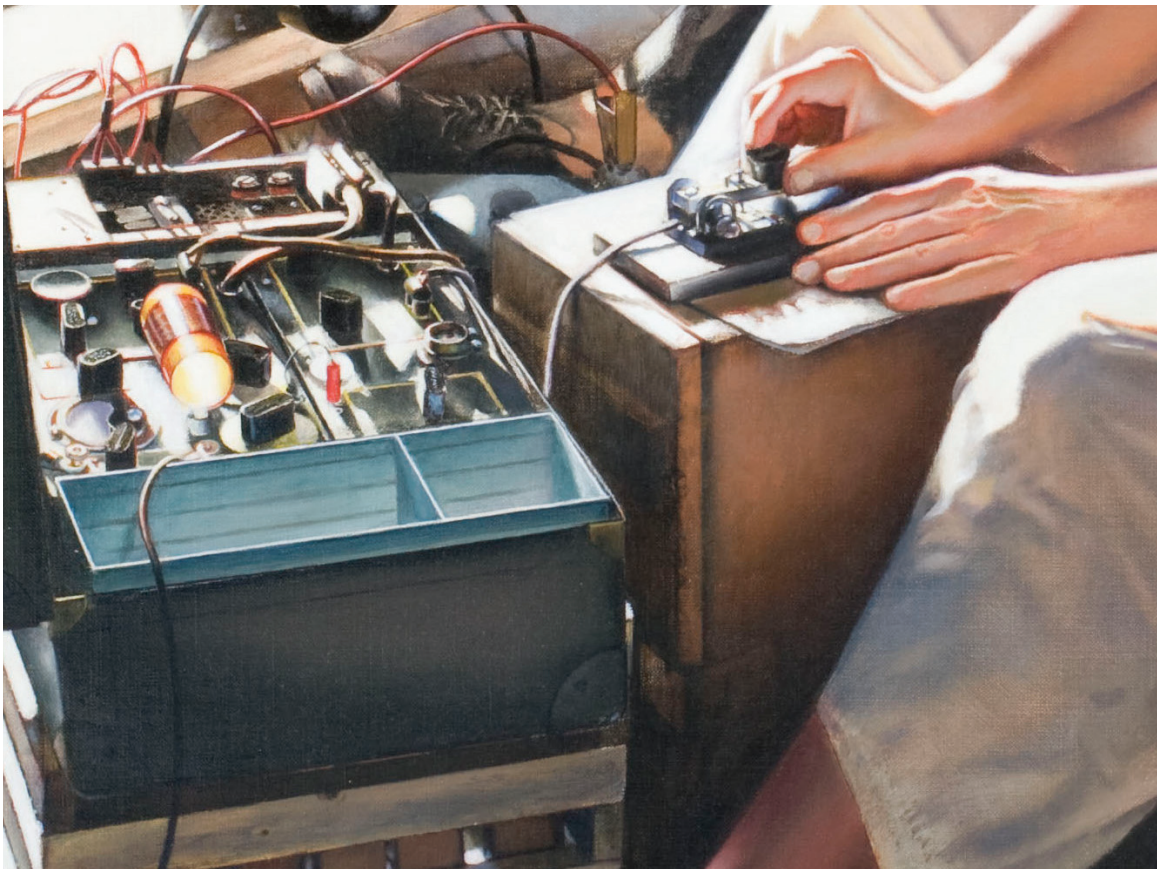
BRIAN AUTEN

INTRODUCTION & BASIC RECONNAISSANCE

Over the last ten years, scholars have shown deeper interest in applying the just war tradition to the *extra bellum* realm, especially to intelligence collection and surveillance. In multiple academic journals, swords have crossed over whether "just intelligence" and "just surveillance" are viable research projects, while a number of books have tried to connect ethics to the world's "second oldest profession." This article compares the ethical frameworks of two specific authors in this project—the late Sir Michael Quinlan and Kevin Macnish—and evaluates their work in light of how the US Intelligence Community (USIC), specifically the FBI, considers *jus in bello* in national security investigations.

The debates over "just intelligence" and "just surveillance" have had a distinctly cross-Atlantic character. Initially, Aberyswyth University's Department of International Politics served as one intellectual springboard. There, beginning in 2002, Toni Erskine and, later, her doctoral student, Ross Bellaby, examined notions of personal agency, responsibility, and harm in intelligence operations. In 2005, Quinlan, who served as a Permanent Secretary in the UK Ministry of Defense, gave a now-canonical lecture to Aberyswyth's Centre for Intelligence and International Security Studies. Later published as an article in *Intelligence and National Security,* Quinlan coined the phrases *jus ad intelligentiam* and *jus in intelligentia*—the analogical application of *jus ad bellum* (just resort to war) and *jus in bello* (just execution of war), respectively, to a state's intelligence operations. Two retirees from the UK Government Communications Headquarters (GCHQ), David Omand and Michael Herman, have made their own contributions to the conversation, the most recent of which is Omand's *Securing the State* (2010).

In the United States, Jan Goldman—a now-retired intelligence professional and professor at Tiffin University—brought together a multidisciplinary coterie in his two-volume anthology *The Ethics of Spying* (2006; 2010). The first volume offered selections from former CIA Director Robert Gates and well-known intelligence scholars like Loch Johnson, Art Hulnick, and David Perry, but also included articles on philosophy, the ethics of interrogation, and the co-opting of anthropologists for national security and defense purposes. Goldman's second volume continued along the same vein, integrating the work done in the UK by Erskine and Herman and including voices involved in Surveillance Studies circles. Goldman's



work would be augmented by James Olson's *Fair Play* (2007); David Perry's *Partly Cloudy* (2009); David Price's *Anthropological Intelligence* (2008), *Weaponizing Anthropology* (2011), and *Cold War Anthropology* (2016); and Darrell Cole's *Just War and the Ethics of Espionage* (2014), which was just reviewed in these pages. Goldman was also the driving force behind the International Intelligence Ethics Association (IIEA)—which held annual conferences between 2006 and 2011—and the short-lived *International Journal of Intelligence Ethics*.

Now, after *l'affaire* Snowden, the just intelligence debate has morphed into a more concerted discussion about the just war tradition and one particular subcategory of intelligence collection—surveillance. Writing in *Studies in Christian Ethics* and *Surveillance and Society*, an online journal of the UK Surveillance Studies Network, the four major names associated with the just surveillance conversation are MIT's Gary Marx, a long-standing surveillance scholar whose work was used in Jan Goldman's second volume; David Lyon, the director of the Surveillance Studies Centre at Queens University (Canada); Eric Stoddart, a lecturer with University of St. Andrews' School of Divinity; and—most pointedly—Macnish, a former GCHQ SIGINT (signals intelligence) analyst and pastor, and currently a lecturer at the University of Leeds. Following in Quinlan's shoes, Macnish has offered his own variant of *jus ad bellum* and *jus in bello* for the world of surveillance: *jus ad speculandum* and *jus in speculando*.

Jus ad intelligentiam & *jus ad speculandum*

Quinlan's *jus ad intelligentiam* and Macnish's *jus ad speculandum* are meant to focus attention on the interplay between intelligence operations and national security investigations (e.g., counterintelligence, counterterrorism, or counterespionage cases) and the traditional deontological and prudential *ad bellum* categories of sovereign authority, just cause, right intention, last resort, likelihood of success, and proportionality of ends (macroportionality). Surveillance being one means of collection in both non-investigatory and investigatory operations, Macnish's *jus ad speculandum* might be more appropriately cast as a species of *ad intelligentiam*; however, both are trying to answer the same questions: Is an intelligence operation, national

security investigation, or act of surveillance being initiated under the proper authorities for the right purposes? Will an intelligence operation, national security investigation, or act of surveillance achieve the good it is meant to? And, in the end, will the expected good be overwhelmed by the resulting harm or damage arising out of the planned operation, investigation, or surveillance act?

Quinlan's *ad intelligentiam* is comparatively sparse with respect to the traditional deontological just war categories of sovereign authority, just cause, or right intention. The state-as-dominant-actor is assumed, and the issues for which the state might wish to initiate collection fall along a spectrum. At one end, there are less-sensitive matters open to non-clandestine means, and on the other, closely-held plans and intentions regarding imminent threats requiring less overt, more invasive approaches. Falling back on the prudential *ad bellum* categories, Quinlan argues that clandestine intelligence collection may be done after an evaluation of, and an attempt to use, some of the more overt methods (i.e., it is to be undertaken as a type of last resort), and may be done only if the attendant harms or damages from clandestine operations would still allow "[a government] to forestall, counter or alleviate actions that would be seriously damaging" to the political community and its citizenry (i.e., macro-proportionality and probability of success).[1]

In contrast, Macnish's *ad speculandum* is more focused on the distinction between *bellum,* the use of force-in-the-form-of-surveillance for the common good of the *polis,* and *duellum*, the private use of surveillance for non-public goals.[2] Not that surveillance is performed solely at the state level—Macnish demonstrates how his model works for the private gumshoe and for a corporation's tracking of "insider threats"—but when it comes to state-authorized surveillance, he is emphatic that one may not use the state's instruments of surveillance to indulge one's private whims and desires, or for "salacious, trivial or ignoble causes."[3] A just cause for a state's use of surveillance would therefore not include the protection of an individual's personal reputation, his financial gain, or his professional advancement, but rather the necessary and "genuine defense of the lives of [the state's] citizens."[4]

"Genuine defense" as a commonsense approach to the concept of necessity in just cause, admits Macnish, is open to abuse. It is a fine enough concept for a state with healthy, functioning firewalls between the public good and private interests, but in regimes without such protections, it might be used to justify the tracking of dissidents or political enemies.[5] Additionally, as Macnish outlines, in both investigatory and non-investigatory scenarios, collection may be necessary to confirm or disprove a hypothesis about the nature of a threat or a competing nation's capabilities. "Genuine defense," then, may necessitate collection based on little more than suspicion.[6] The standard of reasonableness is what guards against impropriety and misconduct in such cases, but it is still an important and oft-overlooked point. Intelligence operations and acts of surveillance contribute to "genuine defense" by confirming the accuracy of reporting streams, refuting longstanding assumptions, and improving the confidence levels of one's existing analytical assessments—but these all may occur on the basis of what might best be deemed reasoned hunches.

Unfortunately, neither scholar's model has enough to say about right intention. The category is simply missing in action in Quinlan's article, while Macnish focuses on ulterior motives and the use of just cause as a "cover" or fig leaf. "[The surveillant must not]," argues Macnish, "pursue an ulterior motive undermin[ing] the value of the just cause" or hide his true inner motives under the public guise of a just cause.[7] I would like to see greater attention by Macnish as to the proper content or character of those motives. Right intention isn't simply just about a mismatch between behavior and inner motivation. In a manner reminiscent of the Apostle Paul's admonitions to believers to "put off" their former, worldly natures and "put on" the Christian virtues, it is about the "putting-off" of selfish or malevolent motivations for action and the "putting-on" of peace through love. Instead of rebellion, vengeance, or the lust for power and glory—motivations embodying what the New Testament labels *epithumia* (*cupiditas*, self-love or, using an older term, concupiscence)—right intention requires *agape* (*caritas*), the Christian's tangible expression of love for one's neighbors and the world.[8] In *jus ad intelligentiam* and *jus ad speculandum*, right intention should therefore connect three things: the sovereign's initiation of an intelligence operation or act of surveillance; the sovereign's guidance as to the types of acts used at the strategic, operational, and tactical levels; and the Augustinian political goal of peace defined as the "order of tranquility" (*tranquillitas ordinis*).

Jus in intelligentia & *jus in speculando*

As is well-known to *Providence* readers, sovereign authority, just cause, and right intention do not necessarily address *how* an individual is to fight in a just manner once a conflict is underway, though one could argue that right intention's requirement of *agape*-motivated behavior towards one's opponents suggests, at the very least, a specific type of demeanor. *Jus in bello* involves judgment as to the just and proper execution of force at the operational and tactical levels of conflict. It is typically explained using the categories of micro-proportionality and discrimination.

Micro-proportionality, or proportionality of means, involves an evaluation as to whether the anticipated harms or evil resulting from a particular operation or use of force will outweigh the expected good. It recognizes that, in a just conflict, there are some applications of force that are unwise because they do not "fit" with the cause at hand and, if pursued, can poison the very possibility of ever arriving at *tranquillitas ordinis*. In his discussion of proportionality writ large in the pages of *In Defence of War*, Nigel Biggar explains that at both levels, proportionality is meant to limit damage and to "[rule] against military operations that appear to be imprudently expensive of human lives." A judgment of disproportion, Biggar goes on to say, is made when the anticipated evil or harm arising out of an action is plainly unnecessary or likely to "subvert or destroy the very good that one hopes to gain by it."[9]

The second *in bello* category is discrimination, the ability to distinguish at the operational and tactical level between those who may and may not be legitimately and licitly attacked. It aims at protecting certain categories of people from harm—women, children, the elderly, and the mentally infirm or disabled. Double effect is an associated concept which allows for the injury or death of those who may not be intentionally targeted if—and only if—such harm is incidental to an action intentionally aimed at a legitimate, military objective.

Micro-proportionality and discrimination are addressed by Quinlan's *jus in intelligentia* and Macnish's *jus in speculando*. Both models ask: at the point of the act itself, who is the proper target, and what are legitimate, just methods of intelligence collection and surveillance? Quinlan highlights key *in bello* concerns about intelligence collection, including the use of coercive versus non-coercive human recruitment and the resort to enhanced interrogation or torture. While lying and deceiving for purposes of covering one's acts are noncontroversial and *de rigueur* for Quinlan, he argues that many aspects of collection run little risk of disproportion or jeopardizing the wellbeing of those who are not legitimate targets. For example, he believes that one may legitimately accept non-public information from a volunteer and perhaps even cajole or tempt an individual to give up secret information. The more coercive the approach, however, or the more innocent the prospective target—Quinlan talks pointedly about the legitimacy of targeting family members or using blackmail and torture—the more potentially illicit is the operation along *in bello* lines. "[T]he line of prohibition [between permissible and impermissible acts of collection]," Quinlan concludes, "might relate to whether serious coercive violence—or its near-equivalent, as in blackmail—is done to individuals whom we are not entitled to harm."[10]

Macnish connects his *in bello* analysis of micro-proportionality and discrimination in surveillance to judgments about threat, harm, invasiveness, and what he calls "liable" and "non-liable" targets. He acknowledges that, overall, surveillance comes in many forms, varies in invasiveness and potential harms, and, as a general rule of thumb, "[the] less extreme the occasion, the less invasive and pervasive the surveillance should be."[11] Surveillance is not life-threatening to the surveilled, but Macnish explains how it can nevertheless result in psychological and social harms, which then play into the overall micro-proportionality calculus. Such harms include but are not limited to individual stereotyping and discrimination (what Surveillance Studies notes as "social sorting"), the discounting of communal and institutional trust, the overwhelming fear of authority, and erosion of privacy.[12] As part of Macnish's discussion on harm, he insists that limiting electronic surveillance to the collection of metadata is comparatively less invasive than the interception and review of content and also references (albeit too quickly) some of the post-*United States vs. Jones* concerns about whether the amount and quality of collected metadata can, upon analysis, build an intimate, personal picture on par with that constructed by collecting and evaluating content.[13]

For the *in speculando* category of discrimination, Macnish contrasts liable and non-liable subjects of surveillance. A liable

LESS INTRUSIVE ACTIVITIES	MORE INTRUSIVE ACTIVITIES
-- Collection of information available from "less sensitive and less protected places" (i.e., open source information, commercially-available data that the public can access)	-- Collection of protected information (i.e., financial data, attorney/client information, material where there is a reasonable expectation of privacy)
-- Collection of information about isolated events and/or locations (i.e., single financial transactions; phone data covering discrete periods; use of a tracking device to detect a single trip; time-limited CCT coverage of a single location)	-- Collection of complete phone call histories, full credit or financial reports, 24/7 physical or electronic surveillance of an individual or group over a wide geographic area, capture of computer file content (versus only host identification information)
-- Collection of information from those who are lawfully entitled to disclose it freely	-- Collection of information from those who, because of the nature of the relationship with the subject of the investigation, have to be compelled legally to give information
-- Interviewing the subject of an investigation away from his/her home, neighborhood or workplace; waiting to interview his or her associates until after an investigation is in the public domain	-- Collecting information in such a way that it increases the probability that the subject and/or the subject's associates will find out about it

Figure 1.

subject is a competent adult who has not given his or her consent to be surveilled, but whose surveillance was, and continues to be, legally authorized. A non-liable subject might be an individual whose surveillance was unauthorized or incidentally collected as part of an authorized operation. Macnish frames it in this way because it is impossible to tie the justness of a particular surveillance act to the nomenclature of "innocent" or "guilty" parties. As he puts it, "the [innocent or guilty] status of the surveilled prior to the act of surveillance is frequently unknown," and as already discussed with respect to *ad speculandum* and legitimate initiations of surveillance, it is often surveillance itself that allows investigatory bodies to reach conclusions about innocence or guilt. For Macnish, double effect concerns non-liable subjects of surveillance. If the particular act of surveillance is legitimately authorized, and the non-liable subject has not been intentionally targeted, any incidental surveillance of the non-liable subject would be morally licit.[14]

NATIONAL SECURITY INVESTIGATIONS & THE "LEAST INTRUSIVE STANDARD"

One way the US Intelligence Community (USIC) addresses Quinlan's *jus in intelligentia* and Macnish's *jus in speculando* when it comes to national security investigations is through the "least intrusive standard." Even after multiple amendments, Executive Order (EO) 12333 has remained clear that when elements of the USIC operate in the United States or are engaged in intelligence collection activities "directed against United States persons abroad," those elements are to use the "least intrusive collection techniques feasible."[15] Because of continued concern regarding potential interference with, or harm to, an individual's privacy, civil liberties, or personal reputation, this standard was reiterated in late 2008 with the release of the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), a set of authorities and procedures addressing all FBI investigational work in the United States, and with the FBI's first Domestic Investigations and Operations Guide (DIOG), the internal policy manual outlining how the FBI operationalizes the AGG-DOM in its everyday investigative policies and procedures.[16]

This does not mean that the FBI is prohibited from using lawful, more intrusive collection techniques, but it does mean that there had to have been consideration and judgment as to micro-proportionality and discrimination. Neither the AGG-DOM nor the DIOG gives a precise definition for "intrusive," but in order to help FBI personnel think through concepts like *jus in intelligentia* and *jus in speculando*, the DIOG lays out a range of typical investigative tactics and techniques which fall along a "more or less intrusive" spectrum.[17] (figure 1)

The FBI DIOG refers to this act of judgment as "balancing the factors" or engaging in a "balancing test" and explicitly ties it to an evaluation of potential harm. In cases where "the threat is remote, the [investigative subject's] involvement is speculative, and the probability of obtaining probative information is low, intrusive efforts may

not be justified (i.e., they may do more harm than good)."[18] If it is judged that the threat is severe or the targeted foreign intelligence is of key importance to US interest or survival, the "feasible" caveat allows for a determination of greater intrusiveness—and therefore the acceptance of a higher probability of injury or harm.[19]

National security investigations are not ethics-free, and therefore many of their parameters comport with the just war tradition—micro-proportionality and discrimination being two. An understanding of *jus in intelligentia* and *jus in speculando* helps remind the investigator that the intrusiveness or invasiveness of his tactics places a subject's reputation, dignity, and privacy at risk and has the ability to cause harm. If an investigation requires interviews of a subject's family, friends, co-workers, or neighbors, or if a pending or ongoing investigation necessitates temporary removal of access to classified information or administrative leave, there is a significant risk of reputational harm and potential injury to the subject's current and future livelihood (e.g., loss of income, negative impact on retirement and health insurance, or questionable marks on one's employment record). Not only that, there is also the relationship between duration and the risk of harm. The more involved the investigation or the longer it continues, the greater the potential opportunities for social and psychological harms and the greater the risks of incidental collection.

In conclusion, when I teach the topic of national security investigations to undergraduates at a Christian college, we cover micro-proportionality, discrimination, and the "least intrusive standard" via a tweaked version of the Golden Rule—namely, if you were being investigated for a national security issue but you knew yourself to be completely innocent, how would you want someone to investigate you? The just intelligence and just surveillance research projects, including Quinlan's and Macnish's models, are meant to provoke thinking along that very same line. P

Brian J. Auten currently serves as a supervisory intelligence analyst with the United States government and is an adjunct professor in the Department of Government at Patrick Henry College in Purcellville, Virginia. All views, opinions and conclusions are solely those of the author and not the US government, or any entity within the US intelligence community. This article was submitted and approved through his agency's pre-publication process.

Endnotes

1 Michael Quinlan, "Just Intelligence: Prolegomena to an Ethical Theory," Intelligence and National Security (Vol. 22, No. 1, February 2007), pp. 7-8.

2 For a discussion regarding bellum and duellum, see James Turner Johnson, "Just War: As it Was and Is," First Things, January 2005.

3 Kevin Macnish, "Just Surveillance? Towards a Normative Theory of Surveillance," Surveillance and Society (Vol. 12, No. 1, 2014), p. 147.

4 Ibid.

5 Ibid.

6 Ibid, pp. 144, 147.

7 Ibid., p. 148.

8 For caritas and cupiditas, see again James Turner Johnson, "Just War: As it Was and Is."

9 Nigel Biggar, In Defence of War (Oxford University Press, 2013), pp. 113-114.

10 Quinlan, pp. 8-11.

11 Macnish, p. 151. Also see Macnish, "Debate: Response," Surveillance and Society (Vol. 12, No. 1, 2014), p. 175, and Macnish, "An Eye for an Eye: Proportionality and Surveillance," Ethical Theory and Moral Practice (Vol. 18, Issue 3, June 2015) [though citation derived from paper manuscript available at academia.edu, pp. 21-22, 24, 31].

12 Macnish, "An Eye for an Eye," manuscript, p. 25.

13 Ibid., p. 27.

14 Macnish, "Just Surveillance," p. 151, and Macnish, "An Eye for an Eye," manuscript, pp. 22-24.

15 US Executive Order 12333, Section 2.4.

16 The Attorney General's Guidelines for Domestic FBI Operations (2008); Domestic Investigations and Operations Guide (16 December 2008; revised version dated 15 October 2011). The first version of the DIOG was declassified with redactions on 8 July 2009; the second was declassified with redactions on 30 August 2011.

17 DIOG, 16 December 2008, pp. 34-38; DIOG, 15 October 2011, pp. 4-15 to 4-18.

18 Attorney General Guidelines, pp. 12-13; DIOG, 16 December 2008, p. 37; DIOG, 15 October 2011, p. 4-18.

19 DIOG, 16 December 2008, pp. 34-38; DIOG, 15 October 2011, pp. 4-15 to 4-18.6.