Chapter 5

Security

Security
Chapter 5

Security
Chapter 5

Introduction
By Fiona de Londras

Over the past year, contributors to the Oxford Human Rights Hub Blog have addressed both direct (e.g. physical and political impacts on victims) and indirect (e.g. on institutional design, use of weaponry and development of international standards) impacts of insecurity from a rights perspective.

'Accountability' is key to ensuring the security state does not infringe on human rights beyond what is necessary and justifiable, however structures of accountability in the counter-terrorist context may not 'look' the same as in other contexts. This is largely because security requires secrecy, and accountability in the face of secrecy requires innovation. The UK innovated in this field by establishing the Independent Reviewer of Terrorism Legislation ('IRTL'), a post now held by David Anderson QC. Writing in March 2014 ('Independent Review of Terrorism Laws: a Brief Introduction' p 92), Anderson acknowledged the challenges of securing public faith in a review, much of the information and reasoning underlying which cannot be disclosed. The key, he argued, was independence. However, in the summer of 2014 the UK government proposed abolishing this office and replacing it with a Privacy and Civil Liberties Board. Jessie Blackbourn expressed concerns about this on the blog in August ('Anti-Terrorism Review Reform: Some Considerations' p 93): how would the panel be appointed? How would it achieve and maintain independence? In the end, the Government decided against abolishing the IRTL and Anderson continues in the role, however other systems have no such office or process. Writing in June 2014, I argued that the EU should introduce *ex post facto* review in order to better understand the impact of these measures ('Accounting for Rights in EU Counter-Terrorism' p 93).

In January 2014, Michele Porcelluzzi drew readers' attention to the deficiencies in UN sanctions regimes from a due process perspective ('The UN Sanctions Regime Against Terrorists: Suggested Changes' p 94). His novel suggestion is that listing and delisting be taken out of the Security Council and done by the International Criminal Court, where 'fair trial' rights could be respected in a manner that recognised the 'criminal justice' nature of the sanctions regime. This is a suggestion that might be taken on board by the Working Groups of the High Level Sanctions Review, which he outlined in a second contribution ('UN Sanctions: Possible Changes?' p 96).

Domestic security measures continued to cause anxiety. Natasha Holcroft-Emmess wrote on Guardian News and Media Ltd v AB & CD [2014] EWCA Crim (B1) where the Court of Appeal acceded to a government request to have a case heard in *camera*, but mandated that some parts should be open (swearing in, reading the charges, the prosecution's opening, the verdicts and sentencing), and permitted a small number of journalists to be present, although they could not report until the trial was concluded ('Partly Clandestine Criminal Trials Risks Standardising Secrecy' p 97). Holcroft-Emmess acknowledged that the Court had to tread a fine line between open administration of justice and protection of sensitive information, but this post highlighted the sharpness of this tension. This sharpness results, not least, from concerns that secrecy may frustrate transparency as well as protect security; a concern I addressed in a post on the Miranda [2014] EWHC 255 (Admin) case ('Managing Secrecy: R (Miranda) v SSHD' p 98). That case, I argued, highlighted the importance of introducing structures to manage secrecy; indeed, that is what Nicol J. was attempting to do in Guardian News and Media Ltd v AB & CD [2014] EWCA Crim (B1).

Closely allied to concerns about secrecy are concerns about privacy, which were prominent in contributions last year. Andrew Wheelhouse wrote on the important decision of the Investigatory Powers Tribunal that 'Tempora' was ECHR-compliant ('The Legality of Mass Surveillance Operations' p 99). Echoing other posts, Wheelhouse raised the challenges of public faith for a system that assesses rights-compliance in largely or wholly closed processes. If Anderson argued that independence is key to maintaining the legitimacy of his role as IRTL, can a Tribunal of this nature claim the same independence? That it can is not at all clear. However, a number of courts did hand down important decisions on privacy, surveillance and the Internet that were analysed on the blog. The Court of Justice of the European Union's (CJEU) decisions on the Data Retention Directive and 'right to be forgotten' were analysed by Menelaos Markakis ('One May Not Retain Personal Data Forever: The Judgment in Google Spain' p 102), who rightly noted the Court's endorsement of a level of judicial scrutiny that "could have hardly been more searching", wide territorial scope for EU data protection, and "very protective" approach to the rights to privacy and protection of personal data. Sinziana Gutiu reflected on the Supreme Court of Canada's decision in R v Spencer [2014] 2 S.C.R. 212 ('The Supreme Court of Canada Affirms Privacy as Anonymity' p 100), finding that privacy can exist as secrecy, as control, and – crucially – as anonymity. Internet users, the Court held, have a reasonable expectation of privacy as anonymity. Melina Padron ('Respect for Private Life under Article 8 and Covert Filming' p 104) brought to readers' attention the European Court of Human Right's decision in Söderman v Sweden [2013] ECHR 1128 in which the Grand Chamber held member states have an obligation to put in place adequate civil and/or criminal provisions to protect individual Article 8 rights, including the right to privacy. In spite of these decisions across various jurisdictions, mass surveillance continued apace; both Australia and the UK introduced data retention legislation, seemingly at odds with the strong form of privacy protection endorsed in particular by the CJEU.

Beyond the context of counter-terrorism and surveillance, the blog also covered important developments in security and rights. Kate Stone marked the entry into force of the Arms Trade Treaty ('Human Rights and the Arms Trade Treaty' p 106), which requires states to consider the likely human rights consequences of arms trades in advance. Stone raises the important question of whether rights can be effectively protected by regulating, rather than preventing, arms trade, but this may be a field in which pragmatism

holds significant promise. While tackling trade in conventional arms, the 'international community' is also faced with a less conventional form of weaponry: drones. In October 2014, Natalie Cargill welcomed the decision of the Human Rights Committee to address this issue head-on (HRCR 25/22), which offered the opportunity to reiterate the applicability of IHL and IHRL to the use of drones, although the Resolution attracted criticism from some states ('"Classic Human Rights Law Territory": Why the HRC Needs to Talk About Drones' p 107). Addressing the use of force against ISIS, Michele Porcelluzzi argued ('Iraq Needs Incisive Measures from the UN Security Council' p 108) that international action, mandated by a Security Council Resolution, was needed in respect of Northern Iraq. However, Security Council Resolutions are useful not only for mandating military intervention, but also for recognising what Sarah Field calls "our shared vulnerability to hurt and harm of unimaginable form and depth", referring to SCR 2139 in Syria ('Dignifying the Most Vulnerable 'In' and 'Through' Security Council Resolution 2139' p 109).

What these contributions to the OxHRH Blog over the past year show is that, while the particularities of debates on security and rights might change with context – review, sanctions, arms trading, secrecy, drones etc–the themes with which we are preoccupied are relatively stable. Efforts to ensure security almost necessarily confound us. On the one hand, security is required for the enjoyment of human rights: we know that situations of insecurity, instability, and the quotidian nature of inter-personal violence severely challenge our capacity to enjoy, and states' capacities to ensure, rights. However, the measures taken in the effort to ensure security themselves pose serous threats to rights. Thus, as the contributions to the blog show, the work of the human rights lawyer and advocate is to critically engage with efforts to understand, 'provide', and review 'security' in order to minimise the challenging tensions that arise.

Prof Fiona de Londras is Professor of Law and Co-Director of the Durham Human Rights Centre at the University of Durham where she coordinates the FP7-funded, collaborative project SECILE. She has spent the 2014-2015 academic year as a Visiting Fellow at Oxford Human Rights Hub.

COUNTER TERRORISM

Independent Review of Terrorism Laws: a Brief Introduction

By David Anderson | 6th March 2014

Monitoring the activities of the secret state creates a conundrum. To be effective, a monitor needs to read and to know what is secret. But why should the monitor be believed, when the monitor's reasoning cannot be shared with the public?

That conundrum is most familiar in the context of intelligence oversight, where the Shadow Home Secretary has recently made some interesting proposals for change. But as she indicated, part of the solution may lie in an older tradition: the independent review of the operation (by police, prosecutors, Ministers and others) of the anti-terrorism laws. Such review has been a feature of the landscape in the UK since 1978 and was adopted in Australia in 2010.

Independent review of terrorism legislation is founded, perhaps quaintly, on trust: the appointment of what was described to Parliament in 1984 as "*a person whose reputation would lend authority to his conclusions, because some of the information that led him to his conclusions would not be published.*"

A second important feature evolved during the tenure of Lord Carlile Q.C., from 2001-2011, as what the Shadow Home Secretary described as a "public-facing form of oversight." However penetrating a review may be, it can neither inform, reassure nor raise the alarm, unless its conclusions are brought, forcibly if necessary, to the attention of Parliament and the general public. This means meeting with the widest possible range of people, giving evidence to Select Committees and accepting a degree of media exposure.

Neither of these features would be worth anything without genuine independence. The Independent Reviewer must set out neither to torment the Government nor to defend it, but to give an informed and considered view. Though not a judge, he or she must always seek to act (in the words of the judicial oath) without fear or favour, affection or ill-will. Successive Reviewers, each of whom has performed the job on a part-time basis and without hope of advancement from Government, have, in my (perhaps not entirely impartial) opinion, been well-endowed with this quality.

As the current Independent Reviewer of Terrorism Legislation, I have sought to explain the history and functions of the post in a working paper, delivered as a lecture to the Statute Law Society on 24 February 2014. I have also traced some of the ways in which the post may affect the decisions made by Government. Topical case studies demonstrate how it may do so both directly and in conjunction with other channels of influence including, most importantly, Parliament and the courts.

David Anderson QC is the Independent Reviewer of Terrorism Legislation and a barrister at Brick Court Chambers.

Accounting for Rights in EU Counter-Terrorism

By Fiona de Londras | 7th June 2014

In the 12 years after 9/11, the EU introduced 239 counter-terrorist measures, 88 of which were legally binding. In the EU, as elsewhere, designing and implementing counter-terrorism carries with it risks for rights.

While a baseline of security is required in order to enjoy rights *per se*, 'countering terrorism' often infringes on the rights of suspected terrorists and, more broadly, undermines social cohesion and the rule of law. For that reason, it is important that we pay proper attention to rights in the making, implementation and review of counter-terrorism laws and policies.

In spite of this, the pre-legislative process in the European Union Constitutional Treaty (EUCT) is problematic from a rights-based perspective, even where the formal ex ante impact assessment process is employed. This process, undertaken by the Commission, engages with stakeholders to predict the environmental, economic and social impacts of proposed measures and provide an evidence-base for political decision-making.

Social impacts include impacts on rights. Understandably, however, the qualitative analysis of rights impact is not easily assessed alongside the quantitative analysis of economic impact, with more 'concrete' data often appearing to receive more analytical weight. Thus, it is not unusual when reading these assessments to notice that the analysis of rights is 'light touch.'

This might be expected, given that forward-looking analyses are speculative, especially in relation to values that are difficult to quantify. But it points toward a need to afford more weight to rights in these assessments, especially as they can also shape later analyses of the 'effectiveness' of measures where such ex post assessment takes place.

We can only ascertain a measure's actual impact once it is operational. Even at that point, it is important to remember that the impact of EUCT will not be uniform across every member state or social group: the vast majority of implementation is national, and there can be significant variations across the member states.

In spite of this, formal *ex post facto* review of EU counter-terrorism is remarkably infrequent, even where the measure in question expressly requires it. Of the 88 legally binding minding measures introduced since 2001, 68 required review, only 33 of which have so far taken place on time (ten have not reached their time limit).

The lack of effective and regular *ex post facto* review of EUCT is highly problematic from a rights-based perspective. The necessity and proportionality of any measure may vary according to changing security and social circumstances and thus requires regular review. Without this, we must rely on the hope that a court will have the opportunity to judicially review a measure to assess its legality, in which assessment is only part of a comprehensive rights-related understanding of the impact of counter-terrorist measures.

The EU is a relative newcomer to counter-terrorism, and although it takes some account of rights, this is not sufficient to ensure EUCT is as rights-compliant as possible. The EU does have the potential to account more fully for rights in its counter-terrorism, in particular by enhancing participation in the life cycle of counter-terrorist law- and policy-making and instigating regular, participatory and evaluative review.

Fiona de Londras is Professor of Law and Co-Director of the Durham Human Rights Centre at the University of Durham where she coordinates the FP7-funded, collaborative project SECILE. She has spent the 2014-2015 academic year as a Visiting Fellow at Oxford Human Rights Hub.

Anti-Terrorism Review Reform: Some Considerations

By Jessie Blackbourn | 8th August 2014

In mid-July, the UK government announced its intention to abolish the Independent Reviewer of Terrorism Legislation – the office tasked to review the UK's anti-terrorism laws – and replace it with a new Privacy and Civil Liberties Board. There is some merit in this proposed reform. A panel of reviewers could mitigate some of the problems in the existing system of review. The current Independent Reviewer, David Anderson QC, is, for example, overburdened with the number of laws he is tasked – as an individual – to review. However, if the Privacy and Civil Liberties Board is to improve on these deficiencies, it must be established according to best practices in government oversight.

The government has not yet outlined the structure of the new Board. This is something to which it must give serious consideration. A panel of reviewers presents a number of problems not found in the current system. How many people will sit on the Board? Will

each member have equal weight? What will be the process if the Board cannot agree? Can individual members write dissenting reports? Recommendations reached by consensus could mean compromise and a decline in the quality of the review. However, a system in which the publication of multiple opinions is allowed could have the same result; indecision will offer scope for the government to adopt the reforms it prefers, rather than the ones that may be most necessary.

The government will also need to consider how it appoints the Board. Anderson was appointed by the Home Secretary in a process which he has described as 'intriguing, if indefensible.' Since then, he has succeeded in making the appointment process more transparent. Future Independent Reviewers were to be chosen by Ministers in 'an open, fair and merit-based process' from a 'list of appointable candidates.' This should be the minimum appointment procedure for members of the new Board. A more preferable process would be to advertise the position in an open competition. The government also needs to think about the length of term and re-appointment procedures. The Independent Reviewer is appointed for three years, renewable up to a period of ten years. Three years is a very short period of time for new appointees to get aboard such a complex area of law. The government might instead give consideration to establishing a system of rolling appointments for non-renewable five-year periods.

The government will then need to consider the Board's terms of reference. As it stands, the Board will be required to advise the government on whether anti-terrorism legislation 'is sufficient to meet the threat and adequately takes account of privacy and liberty concerns.' Given recent revelations about the extent to which government agencies have infringed citizens' right to privacy, it is perhaps understandable that this has been prioritised. However, some of the UK's anti-terrorism laws, such as those that impose Terrorism Prevention and Investigation Measures on persons only suspected (but not convicted) of terrorist behaviours, pose a far greater challenge to other traditional rights.

The government will also need to think about what powers the Board will require. In order to be meaningful, a review must have full access to all relevant information. The Independent Reviewer currently has no statutory power to access material from the intelligence and security services or the government; however, according to Anderson, it has been granted on trust, based on the establishment of strong relationships between the reviewer and those agencies. Anderson has suggested that for the same access to be granted to the Board, it will need to be 'backed both by watertight statutory guarantees and by the full institutional cooperation of agencies.'

Finally, the government needs to consider the Board's reporting requirements. Currently, the government must table the Independent Reviewer's reports to the parliament 'on receipt.' The government may delay publication of the reports for only enough time to ensure that they contain no information which, if disclosed, might prejudice national security. Whilst disclosure is a legitimate concern, the procedure for determining national security information must be transparent. The government should not have final censorship over the new Board's reports. Additionally, the government should be required to provide an official response to the Board, particularly where laws are not subject to annual renewal and parliamentary debate.

These are just some of the factors that will need to be considered when the government proposes its new Privacy and Civil Liberties Board. Otherwise, we will be worse off than the current system of independent review.

Dr Jessie Blackbourn a Lecturer in Politics and Human Rights at Kingston University.

The UN Sanctions Regime Against Terrorists: Suggested Changes

By Michele Porcelluzzi | 15th January 2014

The current UN sanctions regime against terrorists does not secure due process rights. Allowing the International Criminal Court to deal with these cases would be a preferable solution, as it would prevent violations of such rights.

Overview

Two years before the 9/11 attacks, the UN Security Council adopted Resolution Resolution 1267 (1999), establishing a sanctions regime which required all states to impose a range of preventive measures, including asset freezing, international travel bans and arms embargoes on individuals and entities designated by the Sanctions Committee as being associated with the Taliban.

In the following years, with numerous Security Council resolutions, these measures were extended to individuals, groups and entities associated with Al-Qaeda, and there developed an "Al-Qaeda Sanctions List." Further, the Security Council established guidelines for blacklisting and delisting.

Any state may request the Al-Qaeda Sanctions Committee to add names to the Al-Qaeda Sanctions List. The Committee oversees states' implementation of the sanctions measures, maintains the sanction list and considers submissions from states concerning exemptions to asset freezing and travel bans. It makes decisions on listing by consensus of its Members. If consensus cannot be

reached, the matter may be submitted to the Security Council by the member concerned. Finally, a listed person or entity receives a narrative summary of the reason of the listing, which does not include any information that the designating state considers sensitive.

Problems

The sanctions significantly interfere with the fundamental right to freedom of movement, property rights and the right to privacy in all its manifestations. Further, the duration of the sanctions is not determined, so in most cases, it is permanent. The procedure is also entirely political, lacking any judicial control. The Committee is composed of diplomats, rather than independent judges. An individual is not allowed to intervene in the proceedings to prove his innocence and often receives an unduly narrow summary of the decision. There are clear violations of the "fair trial" rights set up by article 14 ICCPR, which depend on the independence of a decision-maker, accessibility and power to grant an effective remedy.

Due to criticism from many commentators, NGOs and UN Member States, in 2009 the Security Council introduced an independent Ombudsperson to assist the Committee in its consideration of delisting requests. The Ombudsperson investigates delisting requests and prepares a "comprehensive report." This report contains formal recommendations to the Committee on whether to accept or reject a delisting request. If the Ombudsperson recommends against retaining a listing, then that individual or entity is delisted within 60 days, unless the Committee decides unanimously to retain it, or the question is referred to the Security Council.

The Special Rapporteur, in his 2012 report, concluded that "*the Al-Qaeda sanctions regime continues to fall short of international minimum standards of due process.*" He suggested extending the powers of the Ombudsperson, whose decision must be accepted as final by the Al-Qaeda Sanctions Committee and the Security Council.

Solutions

In order to uphold due process rights, the best solution would be to bring the listing and delisting procedures within the jurisdiction of the International Criminal Court. This would ensure that decisions are made by independent judges on the basis of clear norms, which would set the standard for cooperation with Al-Qaeda. Further, individuals would be able to intervene in both procedures and challenge the evidence put forward by the states. The Court would also provide a clear and complete reason for its decision in each case. Respecting due process rights would also facilitate the implementation of sanctions in the EU. The ECJ would not itself need to undertake a complete review – such in the Kadi II [2013] EUECJ C-584/10 case, as long as the ICC maintained this elevated standard of protection.

Respecting human rights is a necessary condition for fighting terrorism, as violations of these rights will only create an atmosphere of resentment. The existing regime does not respect human rights to the required extent. However, the suggested amendments could hopefully facilitate their protection.

Michele M. Porcelluzzi completed his M.Sc. in Law at Bocconi University in 2010. His research interests include International Public Law, International Humanitarian Law, Human Rights Law and National Security Law.

UN Sanctions: Possible Changes?

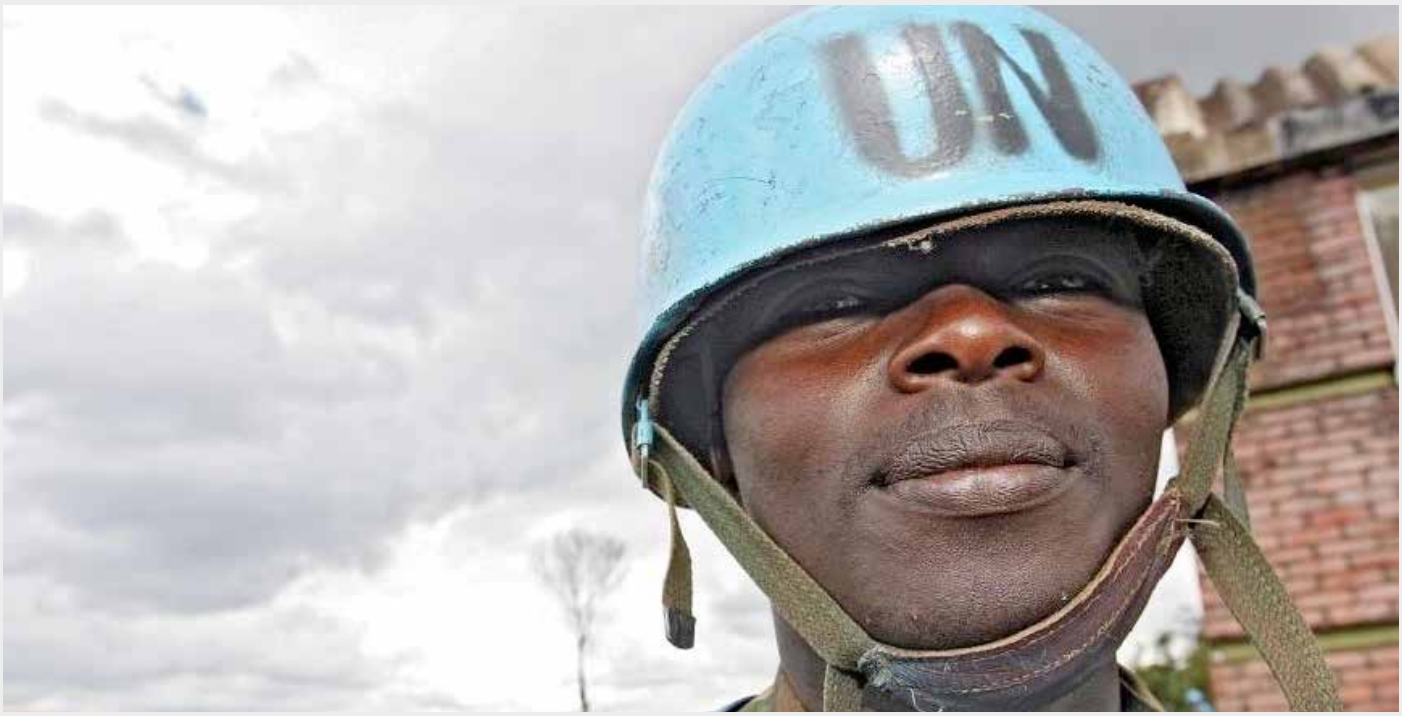
By Michele Porcelluzzi | 24th July 2014

In the last 20 years, the UN Security Council has adopted numerous sanctions not involving the use of armed force.

Originally, these sanctions only targeted States and aimed to prevent or punish cross-border attacks, civil wars and terrorism. They have since narrowed to target specific entities or individuals, and the rationale for sanctions has expanded to include the protection of civilians and prevention of human rights atrocities, the discontinuation of the development of unconventional arms and their delivery systems, and the financing conflict through exploitation of natural resources or criminal activities. For example, the Sudanese sanctions regime, established by Resolution 1591 (2005), imposed measures including travel bans and asset freezing on individuals designated by the Committee.

Today, there are 15 sanctions committees, supported by 65 experts working on 11 monitoring teams, groups and panels, at a cost of about $32 million dollars a year.

There are, however, several problems with the existing sanctions regime. First, some sanctions regimes targeting individuals, such as those against terrorists, do not secure due process and human rights. Furthermore, in order to assure effectiveness, it is necessary to develop strategic partnerships with other control mechanisms or regulatory systems. At the moment, the United Nations cooperates with the International Civil Aviation Organization, the International Maritime Organization, INTERPOL and the World Customs Organization. However, there is a notable absence of collaboration between UN sanctions committees and financial and arms embargo regulatory organs, like those established by the European Union or Organization for Security and Co-operation in Europe.



Moreover, new crisis resolution tools dealing with many of these same threats have been developed; these include mediators, international tribunals and sanctions by entities other than the UN. It would therefore be desirable for UN sanctions to be integrated with these new tools in order to become an integral part of a larger strategy.

In June 2013, a High Level sanctions review was initiated, sponsored by the UN Missions of Australia, Finland, Greece and Sweden, in combination with Brown University and the sanctions consulting firm CCI. A similar activity took place in 2006, with the Informal Working Group on General Issues of Sanctions, which resulted in important policy documents for sanctions regimes.

The current sanctions review is being conducted by sanctions practitioners with extensive experience in the service of their Governments, the Secretariat, international organizations or current and former sanctions monitors. Three Working Groups are addressing different issues.

The first group is dealing with integration and coordination on the implementation of UN sanctions. In particular, it is focusing its attention on opportunities to improve sanctions integration and coordination among the UN entities supporting the Council's sanctions function, including sanctions committees, expert groups, the Ombudsperson and the Secretariat.

The second Working Group is addressing the possible partnerships and strategies between the UN sanctions regime and other international instruments and institutions dealing with international security, such as international arms control and disarmament mechanisms, international financial and economic regulatory systems and international criminal justice institutions.

The Third Working Group is focusing its attention on UN sanctions, regional organizations and emerging challenges. In particular, it is addressing opportunities to optimize UN sanctions as an effective tool in response to serious and systematic violations of human rights and international humanitarian law, enhancing coordination with regional sanctions and exploring new applications to address evolving threats to international peace and security.

This review of UN sanctions is indispensable and may be very useful if it is conducted periodically, for example, every five years. However, there are two obstacles, which Working Groups may face. First, the operations of the UN sanctions regime and the International Criminal Court often overlap. More coordination between these bodies may therefore be required.

Secondly, the Working Groups need to address the perceived lack of respect for due process rights by the UN sanctions regime. The European Court of Human Rights in Nada and the European Court of Justice in Kadi, as well as some domestic courts, have challenged the regime against terrorists on due process grounds.

Despite these problems, it is hoped that the Working Groups, whose activity will conclude in October 2014, will nonetheless provide a useful and meaningful review of existing sanctions regimes.

Michele M. Porcelluzzi completed his M.Sc. in Law at Bocconi University in 2010. His research interests include International Public Law, International Humanitarian Law, Human Rights Law and National Security Law.

Partially Clandestine Criminal Trials Risk Standardising Secrecy

By Natasha Holcroft-Emmess | 15th June 2014

In the case of Guardian v AB and CD [2014] EWCA Crim (B1), handed down 4 June 2014, the UK Court of Appeal addressed the issue of secrecy in criminal trials on the grounds of national security.

UK Government Ministers requested that a criminal trial be conducted entirely behind closed doors and that the defendants be anonymised. The trial judge acquiesced to the request, but the Court of Appeal overturned this in part. It is submitted that the decision does go some way to preserving the interest in the public administration of justice, but some unease remains, and courts ought to be apprehensive of accepting any in-roads into open justice.

Two defendants are facing multiple criminal charges of (mostly inchoate) terrorism offences. On 19 May 2014, the trial judge, Nicol J, ruled that the entirety of the criminal trial could take place *in camera* (i.e. in private, to the exclusion of the public and the media) and that the defendants' identities could be withheld from publication.

The prosecution adduced ministerially-endorsed Certificates setting out reasons in favour of conducting the criminal trials in secret. The justification centred upon preservation of national security. Various representatives of the media appealed the trial judge's decision to permit the trial to go ahead completely *in camera* and to censor any publication of the names of the accused.

The Court of Appeal decided that the evidence available to it indicated a significant risk that the administration of justice would be frustrated if the trial were conducted in open court. As a result, the core of the trial could be held *in camera*. However, some parts of the trial could be conducted in open court, namely: swearing in of the jury, reading of the charges, the judge's introductory remarks, the prosecution's opening, the verdicts and (if applicable) sentencing.

The Court of Appeal also decided that a small number of accredited journalists could attend the bulk of the trial (subject to exclusion from discussion of some matters in accordance with the Certificates) on terms of confidentiality until a review at conclusion of the trial.

On the other hand, the Court of Appeal could not countenance conducting part of the trial in secret and anonymising the defendants. The defendants could therefore be named as Erol Incedal and Mounir Rarmoul-Bouhadjar. The reasons for this will be substantiated in forthcoming judgments. An early indication of the court's approach appears in the introduction, which describes the

Rule of Law as a priceless asset and foundation of the UK's Constitution. One aspect of the Rule of Law is open justice: trials being held in public and the names of defendants publishable. This fundamental principle of the common law ensures public confidence in the legal system. Justice must not only be done but also seen to be done.

The Court of Appeal decision is agreeable in that it emphasises the need for adequate justification for departures from the principle of open justice. It expressly limits such departures to circumstances of necessity and requires a proportionality analysis to be undertaken. The court's vigilance concerning the cumulative effects of various in-roads into open justice is encouraging.

But the fundamental tension between the public interest in national security and the public interest in the open administration of justice remains. The case was described as exceptional, and the need for some secrecy was determined as justified on the facts of the case. Although it is ultimately for courts to decide whether to give effect to a Certificate advocating secrecy in the interests of national security, the judges appear to adopt an openly deferential stance to ministerial urging.

It is argued that the courts ought to be especially vigilant of the risks of accepting any intrusions into open justice and fair trial rights, not just the cumulative effect of many. This is an area in which a quantitative assessment of the impact of multiple incursions, although to some extent helpful, risks undermining the cause of open justice by permitting several small in-roads and standardising a certain amount of secrecy.

Natasha Holcroft-Emmess is a London-based solicitor. She completed the BCL with distinction and is a frequent contributor to the Oxford Human Rights Hub Blog.

MASS SURVEILLANCE

Managing Secrecy: R (Miranda) v SSHD

By Fiona de Londras | 19th February 2014

Much has already been written about the implications of R (Miranda) v Secretary of State for the Home Department [2014] EWHC 255 (Admin) for Schedule 7 Terrorism Act 2007. However, leaving that to one side, I want to reflect on the questions about secrecy that Miranda touches on.

Although some have criticised the judgment for equating investigative journalism with terrorism, Laws LJ held that "[t]here is no suggestion that media reporting on terrorism ought *per se* to be considered equivalent to assisting terrorists." However, some disclosures made by journalists might have the effect of aiding or assisting terrorists in evading counter-terrorism. That may be an unpopular proposition but it is likely correct, and it raises important questions about where the legitimate lines between secrecy and transparency lie and who gets to decide when they have been crossed.

Secrecy and counter-terrorism go hand in hand. Complete transparency (i.e. disclosure of all activities to the public at large) when it comes to counter-terrorism is neither practicable nor desirable from a security perspective. That is not to say that absolute secrecy is necessary or desirable either. Instead, cases like Miranda should cause us to think about secrecy – and, as a result, transparency – as a layered phenomenon.

1. Broadly drawn and simplistically described, there are at least four layers of secrecy/transparency that we might think about in the counter-terrorist context.
2. Public public: elements of counter-terrorism that are publicly known and deliberated upon, such as legislative frameworks.
3. Public political: elements of counter-terrorism that are not subject to full public disclosure but which are disclosed to the public through the *proxy* of political actors. Here there is public scrutiny through representative politics but not through full public deliberation.
4. Private political: there is disclosure to some political actors, but that disclosure is not subjected to political scrutiny within traditional parliamentary structures. This might include private security briefings and disclosures to relevant ministers.
5. Agency private: where disclosures happen within the relevant agency or agencies, and there is limited or no political disclosure.

In many cases, all four of these levels coexist. However, in other cases–such as in relation to the disclosures flowing from Edward Snowden's whistle blowing – there is little or no 'public public' or 'political public' information. Instead, the existence and detail of the counter-terrorist activity in question are almost completely secret. This poses serious democratic and legitimacy concerns that whistleblowers and journalists try to manage.

In essence, the question that Miranda raises is whether journalistic expression that attempts to manage these secrecy concerns through disclosure ought to be protected to the extent of being exempted from laws and structures that are designed to protect

security. Laws LJ was obviously skeptical. At paragraph 58 he wrote, of Greenwald's account of how disclosure decisions are made:

…the reader is left in the dark as to how it is that "highly experienced journalists and legal experts" … are able to know what may and what may not be published without endangering life or security… [T]he journalist may not understand the intrinsic significance of material in his hands; more particularly, the consequences of revealing this or that fact will depend upon knowledge of the whole "jigsaw" (a term used in the course of argument) of disparate pieces of intelligence, to which [journalists] will not have access….

This passage raises legitimate concerns, but it also implicitly emphasises the importance that we ought to attach to constructing appropriate structures for the management of secrecy. If it is true that journalists – even with legal advice – cannot fully appreciate the security implications of disclosing secret counter-terrorist operations and information, then at the very least, we should be able to expect that we would have transparency under headings 2, 3 and 4 above (i.e. public political, private political and agency private) in respect of all security activities.

Journalism, which creates 'public public' transparency, may not always have the capabilities to make the kinds of security judgements necessary to assess whether a particular piece of information ought to be in the public domain, but neither ought we allow security agencies to monopolise both the information that we use to assess threats and the decisions as to disclosure.

Fiona de Londras is Professor of Law and Co-Director of the Durham Human Rights Centre at the University of Durham where she coordinates the FP7-funded, collaborative project SECILE. She has spent the 2014-2015 academic year as a Visiting Fellow at Oxford Human Rights Hub.

The Legality of Mass Surveillance Operations

By Andrew Wheelhouse | 7th February 2015

A court, which isn't a court in name, rules on the legality of a government mass surveillance program that may or may not exist. That about sums up the Kafkaesque world inhabited by the UK's Investigatory Powers Tribunal in Liberty v GCHQ [2014] UKIPTrib 13_77-H.

This claim arose out of the revelations by former National Security Agency (NSA) contractor Edward Snowden and fell into two parts: first, that GCHQ (The UK's signals intelligence agency) had unlawfully been supplied information obtained through the NSA's 'Prism' program; second, that GCHQ had been running its own unlawful mass surveillance program, named 'Tempora.' A variety of civil liberty NGOs alleged that these activities breached the right to privacy under Article 8 of the European Convention on Human Rights (ECHR) and collaterally breached the right to freedom of expression under Article 10 (through the 'chilling effect' on organisations that believe their communications are possibly being monitored).

The British government will neither confirm nor deny the existence of Tempora. The hearing therefore proceeded, somewhat

bizarrely, on the basis of 'alleged factual premises' for five days, with a one-day closed hearing from which the claimants were excluded so that the Tribunal could consider material deemed too sensitive to be heard in public.

Surveillance and communications interception in the UK is governed by the Regulation of Investigatory Powers Act (RIPA) 2000. Under s.8(4) RIPA, an interception warrant issued by a Minister is required for public authorities to carry out surveillance. Information passed to GCHQ by the NSA is governed by a hodgepodge of other statutory provisions.

The Tribunal considered that compliance with the ECHR essentially boiled down to two questions:
- Are there publically known rules for the interception of communications whose content is sufficiently indicated?
- Are these rules subject to proper oversight?

On the first point they were satisfied that the (classified) arrangements for implementing the statutory framework sufficiently restricted the potential for abuse of the surveillance system. Although these arrangements were not themselves known, this defect was remedied by the statutory bodies that oversee the system, namely the Intelligence and Security Committee of Parliament and the Interception of Communications Commissioner. Their reports are available to the public and indicate enough about the rules governing interception to ensure the programme's lawfulness.

On the second point, these bodies, combined with the IPT, provide sufficient oversight of the programme to ensure its legality. Accordingly, GCHQ had, in principle, acted lawfully (or would be, hypothetically). Prism and Tempora take us to the bleeding edge of intelligence gathering in the information age, and it is highly debatable whether Article 8 permits the gathering of 'Big Data' for storage in vast databases. This will no doubt be tested in the separate challenge to Tempora currently before the ECtHR in Strasbourg.

Especially troubling is the use of closed hearings resulting in judgments that do not tell the whole story. British judges may well rigorously scrutinise the work of the security services, which may well be entirely candid in the evidence they present behind closed doors. We have no idea. But we note the recent abuse of RIPA by police to hack the phone records of journalists and the tendency of those tasked with scrutinising the security services to suddenly change their tune when presented with classified information.

The latter point helps explain the muted public reaction to Tempora. Who cares about GCHQ collecting your Whatsapp messages that they will probably never read when national security is at stake? The public is alarmed by the prospect of 'lone wolf' terrorist attacks on British soil, particularly if and when disaffected Britons, currently fighting for IS, return. Bluntly speaking, news of Charlie Hebdo brought crowds out onto the streets. News of Tempora did not.

Secret judicial processes and mass surveillance are an affront to the idea of open justice in a free society. They are also an indictment of a society that has been unable to culturally confront home-grown Islamic extremism, leaving a vacuum filled by the authoritarian application of state power. In the aftermath of Charlie Hebdo, this is changing. In the meantime, we will be forced to endure laws that undermine the very values we claim to fight for.

Andrew Wheelhouse was called to the Bar Of England & Wales at Middle Temple in 2013. Between January and July 2014 he served as a Foreign Law Clerk to Justices Skweyiya and Madlanga at the Constitutional Court of South Africa. He writes here solely in a personal capacity.

The Supreme Court of Canada Affirms Privacy as Anonymity

By Sinziana Gutiu | 5th July 2014

This is a critical time for privacy on the Internet. Private entities, from the global, all-knowing Google to a local Internet Service Provider (ISP), retain sensitive and private information about their users. In Canada, privacy advocates are concerned about Bill C-13, the "*Cyberbullying Act*" and Bill S-4, the *Digital Privacy Act*, which are currently before Parliament and which can have serious privacy implications for Canadians. The Supreme Court of Canada's landmark decision in R v. Spencer 2014 SCC 43, which affirms anonymity as a key component of the right to privacy, comes at a much-needed time.

Mr. Spencer accessed and stored child pornography by way of the free peer-to-peer file-sharing program LimeWire. By using publicly available software, the Saskatoon Police Service was able to obtain the Internet Protocol address of the computer but needed more information in order to identify the individual user. Police investigators made a written "law enforcement request" for the subscriber information pursuant to s.7(3)(c.1)(ii) of the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) to Shaw (the ISP), who complied with the request and released the name, address and telephone number of the customer using the IP address. The police used this information to obtain a search warrant, search Mr. Spencer's home and seize his computer, which contained hundreds of child pornography images.

The Supreme Court of Canada was faced with a number of questions, including whether, in the circumstances, the police conduct violated Mr. Spencer's s.8 Charter right to privacy.

The Court looked at the subject mater of the search, the nature of the privacy interest triggered by the search, and whether Mr. Spencer had a reasonable expectation of privacy in the personal information disclosed by Shaw. The Court found that Mr. Spencer's name, address and telephone number did not simply provide the information of someone who had a contractual relationship with Shaw, but rather, linked information about the identity of an internet subscriber to a particular internet usage, which could reveal intimate details of the lifestyle and personal choices of an individual.

In assessing the nature of the privacy interest, the Court recognized three understandings of informational privacy: privacy as secrecy (e.g. confidentiality of medical information provided by patients), privacy as control (the ability to choose what happens with one's personal information), and privacy as anonymity (where information provided can be disseminated, but without disclosing the identity of its source).

Deciding whether Mr. Spencer had a reasonable expectation of privacy required the Court to look at the provisions of PIPEDA, the federal legislation that creates a general prohibition on the disclosure of personal information without consent. Section 7(3)(c.1)(ii) contains an exception to the requirement for consent when a government institution, for the purpose of law enforcement, makes a request that identifies "its lawful authority to obtain the information."

The Court found that it is reasonable for an internet user to expect that a simple request by police would not amount to lawful authority, would not trigger an obligation to disclose personal information and would not defeat PIPEDA's general prohibition on the disclosure of personal information without consent. The requirement for lawful authority meant that the police could ask Shaw for information but, without a warrant, had no legal authority to compel Shaw to comply with their request.

In conclusion, the Court determined that the police conduct amounted to a "search," triggering Mr. Spencer's s.8 Charter right to privacy and that the search was conducted without lawful authority, but the evidence of the electronic files containing child pornography could not be excluded from the record because of the serious nature of Mr. Spencer's crime, and excluding the evidence would undermine societal interests and put the administration of justice into disrepute.

The decision is a victory for privacy rights. It confirms that Internet users have a reasonable expectation of privacy in their online activities and that anonymity is a critical component of informational privacy. It also clarifies that where privacy statutes require "lawful authority," organizations are empowered to deny warrantless investigative requests and prioritize their customers' privacy interests. In an increasingly public internet space, the decision affirms that individuals have the right to preserve their freedom from identification and surveillance.

Sinziana Gutiu is a litigation associate in the Vancouver office of Dentons Canada LLP.

CJEU Holds the Data Retention Directive Invalid

By Menelaos Markakis | 14th April 2014

In joined cases C-293/12 and C-594/12, the Court of Justice of the European Union ruled that Directive 2006/24/EC on the retention of data by service providers for the purposes of investigating, detecting and prosecuting serious crime was invalid.

There was a disproportionate interference with the right to respect for private life and with the right to the protection of personal data, enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union respectively.

Based on Article 114 TFEU, Directive 2006/24 lays down an obligation on providers of publicly available electronic communications services or of public communications networks to retain certain data generated or processed by them to make it available for the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. This Directive applies to all traffic and location data and to related data necessary to identify the subscriber or registered user. Member states had to ensure that service providers retained data concerning fixed network telephones, mobile telephones, Internet access, Internet e-mail and Internet telephones, which are necessary to identify the source, destination, date, time, duration and type of communication, as well as the users' communication equipment and its location, for up to two years. This data could only be provided to the competent national authorities in accordance with the procedures and conditions laid down by national law.

Having established that there was an interference with Articles 7 and 8 of the Charter (paras. 32-37) and that that interference satisfied an objective of general interest insofar as it 'contribute[s] to the fight against serious crime' (paras. 41-44), the Court turned its attention to the thorny issue of whether the interference was proportionate. In view of the nature of the rights at issue and the extent and seriousness of the interference with those rights, the Court held that 'the EU legislature's discretion is reduced, with the result that review of that discretion should be strict' (paras. 47-48).

The Court noted, first, that the Directive covered all traffic data concerning all means of electronic communication and all subscribers and registered users, thereby entailing 'an interference with the fundamental rights of practically the entire European population' (para. 56). In this connection, it further noted that the Directive did not require any relationship between the data retained and a threat to public security (paras. 58-59).

Secondly, it pointed out that the Directive did not contain any substantive or procedural conditions for access to the data retained by competent national authorities, nor for their subsequent use (paras. 60-62).

Thirdly, the Court noted that no distinction was made on the basis of the potential usefulness of the data retained for attaining the objective pursued or according to the persons concerned (paras. 63-64).

In view of all the above, the Court held that 'Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter,' thereby entailing 'a wide-ranging and particularly serious interference with those fundamental rights' (para. 65). The Court further held that 'Directive 2006/24 does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data' (paras. 66-68).

In view of all these considerations, the Court concluded that the EU legislature had breached the principle of proportionality (para. 69) and ruled the Directive invalid.

From the standpoint of fundamental rights, an academic lawyer would readily notice and welcome the high intensity of review applied and the detailed reasoning provided by the Court in this case. Judicial review could have hardly been more searching. Furthermore, from the standpoint of the EU's competence, respect for fundamental rights, as interpreted by the Court, might sometimes require the Union legislator to harmonise rules in a more detailed manner to limit interference with Charter rights to what is strictly necessary for the attainment of the objective pursued. This presents an interesting juxtaposition between prescribed competence limits and the need to adequately protect fundamental rights when the existence of Union competence is established.

Menelaos Markakis is reading for a DPhil at the University of Oxford and is an Academy of Athens scholar. He is a frequent contributor to the OxHRH Blog.

One May Not Retain Personal Data Forever: The Judgment in Google Spain

By Menelaos Markakis | 29th May 2014

The Court of Justice of the European Union recently held in Google Spain that an individual may, in some cases, request that Google take down personal information from its search results.

The dispute in the main proceedings concerned a decision by the Spanish Data Protection Agency, ordering Google to remove personal data relating to Mr Costeja González from its search results. These concerned an announcement of a real-estate auction connected with the recovery of social security debts, which had appeared on a Spanish newspaper's website upon order of the Ministry of Labour and Social Affairs to attract as many bidders as possible. The announcement was made in 1998, and the attachment proceedings had been fully resolved.

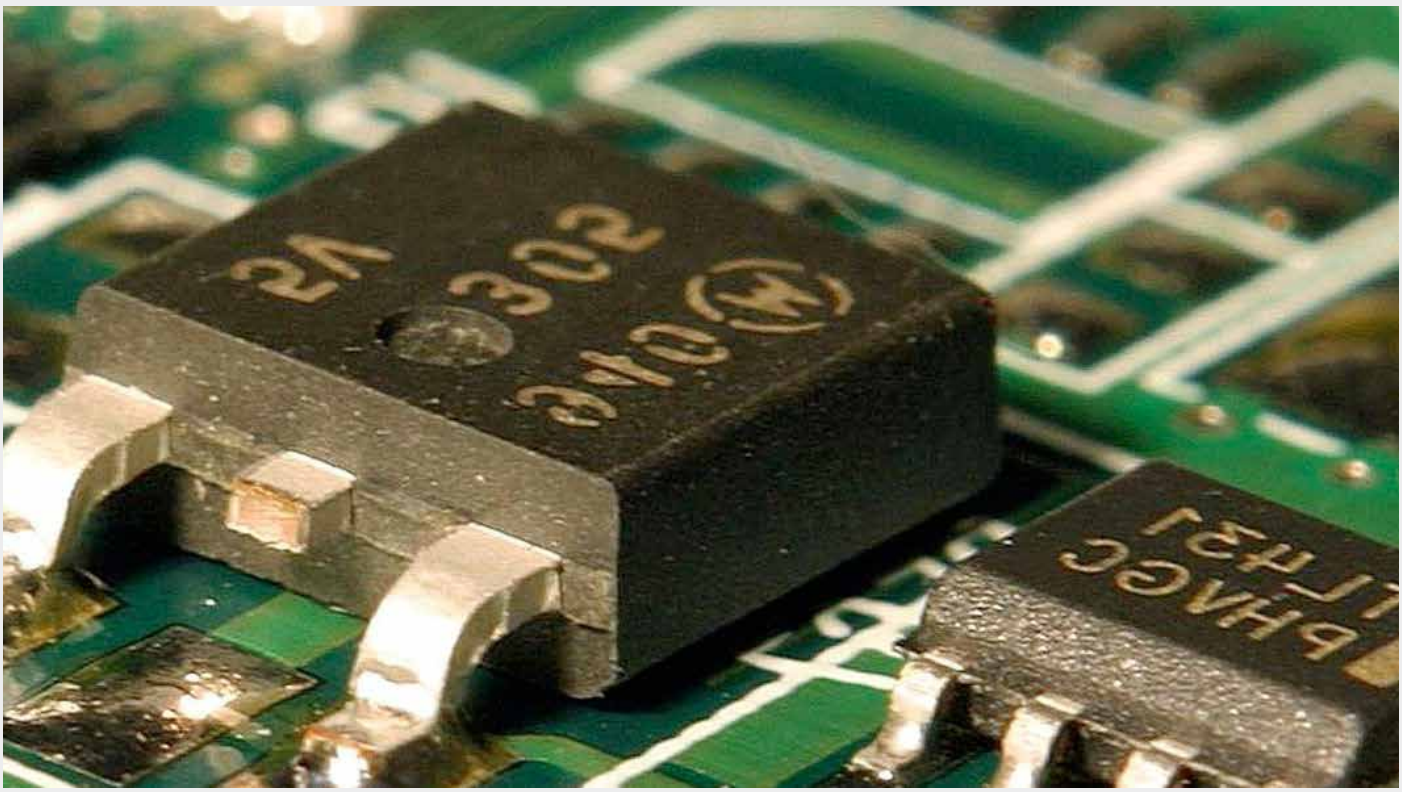
Having established that Directive 95/46 on the protection of individuals with regard to the processing of personal data applies to search engines (paras. 21-41), the Court ruled that the processing of personal data at issue in the main proceedings fell within its territorial scope, even though Google Inc. has its seat in the United States. Relying on the wording of the Directive and on its objective of 'ensuring effective and complete protection of the fundamental rights and freedoms of natural persons,' the Court ruled that the establishment of a Spanish subsidiary (Google Spain) with the purpose of selling advertising space on Google to Spanish clients sufficed to bring the processing within the territorial scope of the Directive (paras. 45-60).

In the absence of any other legitimate ground for the processing of these data, Google had to establish that it was 'necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject' (Article 7(f) Directive). In this connection, the Court noted that the processing of personal data by a search engine 'is liable to affect significantly the fundamental rights to privacy and to the protection of personal data' (Articles 7 and 8 of the Charter of Fundamental Rights of the European Union), in that it 'enables any internet user to obtain … a structured overview of the information relating to that individual that can be found on the internet … and … to establish a more or less detailed profile of him' (para. 80). It was held that, due to the potential seriousness of that interference, it could not be justified by economic interests (para. 81).

Moreover, a 'fair balance' should be sought between the legitimate interest of Internet users in having access to that information, and the fundamental rights of the data subject (para. 81). Whilst the data subject's rights would override, 'as a general rule,' the interest of Internet users, that balance may depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information. This interest could vary according to the role played by the data subject in public life (para. 81). Interpreting the data subject's rights in light of the fundamental rights to privacy and to the protection of personal data, the Court held that he or she 'may … request that the information in question no longer be made available to the general public by its inclusion in such a list of results' (para. 97).

Two points are of particular importance. First, the territorial scope of EU data protection legislation has been ruled to be particularly broad. This development is to be welcomed from a data protection perspective. Second, similarly to the data retention case, the Court appears very protective of the right to respect for private life and the right to the protection of personal data. The impugned data had been lawfully processed by the newspaper and were, above all, true. However, an individual may still, in some cases, request that such information be 'consigned to oblivion,' without having to establish that such processing 'causes prejudice' to him or her (para. 96) or to first request that the original website take it down (paras. 82-88). This seminal judgment marks another step towards the creation of a fully-fledged EU Charter jurisprudence.

Menelaos Markakis is reading for a DPhil at the University of Oxford and is an Academy of Athens scholar. He is a frequent contributor to the OxHRH Blog.



Will Australia Learn from the EU's Mistakes on Data Retention?

By Fiona de Londras | 9th August 2014

Police officers, anti-terrorism officials and politicians all tell us that we need data retention laws, especially in a time of increased technological sophistication. This week, George Brandis, the Attorney General for Australia, announced that Australia will this year join the states with data retention laws, requiring all telecoms providers to retain metadata for two years.

This decision is striking in the light of recent decisions by EU and national courts finding such laws to be disproportionately intrusive on individual rights. Until April of this year, the EU's Data Retention Directive required data retention for between 6 and 24 months in all member states. The proposal for data retention laws had bubbled under the surface of EU politics for some years, but it was not until the London and Madrid bombings that it secured sufficient political support, and it was introduced in 2006. It was, however, controversial right from the start, with civil society being highly critical of its 'catch all' approach to retention, the discretion it left to national states in terms of implementation and the very long retention periods in some EU member states.

In April 2014, the CJEU struck this law down on the basis that it interfered disproportionately in the rights of those within the EU; while data retention was introduced for legitimate security purposes, the Directive simply went too far. In this, the Court was echoing the findings of a number of national courts across the EU, which had also expressed dissatisfaction with the Directive. The concerns raised by the Court in that case offer cautionary tales for Australia at this time.

Importantly, the Court expressly recognised that the data retention model in the Directive–and the model to be introduced in Australia–constitutes blanket surveillance. Once this law is introduced, the data of every single one of the 23 million Australians who use telecommunications devices would be retained and could then be accessed by the government. This is so whether one has ever done anything to arouse suspicion or not; simply using a phone or the Internet will be enough for one's data to be retained. This is problematic in itself but also makes clear the importance of ensuring that the state can only access this information for good faith serious criminal investigations with a court order, where a sound case for access has been made out.

The proposed retention period of two years is extremely long in light of available evidence about when data is usually accessed by states. Across the EU, the majority of requests for access to this data took place within six months of its retention. Why, then, is a two-year retention period being proposed? Have there been cases where the security services and police needed, and could not secure, access to such data as long as two years after the communication in question? And will this be the retention period for everyone, or will people with criminal records (for example) have their data retained for longer than people who have never come to the attention of the state? These questions are fundamental to the proportionality of the law itself.

Metadata can help to make states more secure; however, the mass collection of such data can also make citizens less secure. Telecommunications companies are not necessarily fully equipped to secure the data it holds from accidental release or, indeed, from malicious attacks by hackers and criminal entities. Furthermore, metadata can reveal deeply personal details about our individual lives. Australian politicians and civil society must ask themselves whether, in a country without a comprehensive bill of constitutional rights, this is a step they are prepared to take.

Governments are notoriously reluctant to provide hard facts to back up their plans for new anti-terrorism laws. However, when a government proposes introducing a law the likes of which have been struck down on human rights grounds in numerous states, evidence of its necessity must be demanded. So too must the government prove that the law being proposed contains safeguards showing Australia has learned from the mistakes of other countries. Blanket surveillance hands enormous power to the government. It must show it is prepared to exercise it only within strictly drawn limits.

Fiona de Londras is Professor of Law and Co-Director of the Durham Human Rights Centre at the University of Durham where she coordinates the FP7-funded, collaborative project SECILE. She has spent the 2014-2015 academic year as a Visiting Fellow at Oxford Human Rights Hub.

Respect for Private Life under Article 8 and Covert Filming – Söderman v Sweden

By Melina Padron | 7th January 2014

The Grand Chamber of the European Court of Human Rights ("GC") found Sweden had breached its obligations under Article 8 of the European Convention on Human Rights ("ECHR") for failing to have in place laws protecting the applicant from being filmed without consent.

The case was brought by Ms Söderman, who in 2002 (at age 14) discovered that her stepfather had hidden a recording camera in the bathroom in an attempt to film her naked. The video was quickly destroyed by her mother.

The stepfather was prosecuted for sexual molestation but acquitted by the Swedish appeal court on the grounds that the conduct

lacked an essential element, namely the intention that Ms Söderman find out about the recording. The appeal court noted that Swedish law did not prohibit the filming of individuals without their consent and further, that in theory, his conduct may have constituted attempted child pornography. However, it declined to consider this given the absence of such charges.

Ms Söderman brought a civil claim for compensation in conjunction with the criminal prosecution, but as a result of the acquittal, this claim was dismissed.

She made an application under Article 8 (right to respect for private life) of the ECHR arguing Sweden had failed to provide her with civil or criminal remedies against her stepfather's secret filming, violating her personal integrity.

The Chamber decided by a majority that there had not been a breach of Article 8.

It found that although the crime of sexual molestation did not cover such acts as the one carried out by the stepfather, the crime of attempted child pornography, in theory, could. It also found that other civil remedies were available to Ms Söderman and that it was her choice to join her civil claim to the criminal prosecution. None of these factors amounted to "significant flaws" in Swedish legislation.

The GC overturned the decision of the Chamber and held that there had been a breach of Article 8.

Following the case of M.C. v Bulgaria (Application No 39272/98), the GC noted that the "significant flaws" test had been incorrectly applied by the Chamber as it relates to the assessment of shortcomings in investigations. Instead, the correct test involved considering the adequacy of Sweden's legal framework in providing protection to Ms Söderman against the acts of her stepfather.

The GC heard submissions on whether the secret filming in this case could have constituted attempted child pornography and was not convinced it could have. It found that this provision did not intend to criminalise all pictures of naked children.

The GC considered that the provision on sexual molestation, which in 2002 contained the requirement of intention or recklessness on the part of the offender that the victim find out, had not protected Ms Söderman against the lack of respect for her private life.

Finally, no other provision of Swedish criminal law at the time could have protected her rights under Article 8.

As regards her claim for compensation, the GC was not persuaded that she would have succeeded in pursuing other civil claims said to have been available to her.

This gap in protection left by the absence of both criminal and civil remedies in this case led the GC to conclude that Swedish law in force at the time did not adequately protect Ms Söderman's Article 8 rights. However, the Court recognised that the State had a margin of appreciation on how to afford such protection, and it needed not be solely by the enacting of criminal offences.

The facts of this case are very specific, but this judgment is nevertheless of wide implication. It is bound to send chills up and down the spines of the UK press, especially the tabloids. Whilst it can provide further momentum for those who advocate stronger ethical

parameters in the way the press conducts its work, it should be approached carefully (as it was in Sweden during the process of adoption of new legislation) for its potential detrimental impact on press freedom.

Melina Padron is currently a pupil barrister at Doughty Street Chambers. She was previously a paralegal in Leigh Day's clinical negligence department, a legal caseworker at the AIRE Centre and a visiting lecturer in International Human Rights Law at the University of Bedfordshire.

CONFLICT

Human Rights and the Arms Trade Treaty

By Kate Stone | 9th January 2015

The Arms Trade Treaty (ATT) was adopted by the UN General Assembly on 2nd April 2013. This post marks the recent entry into force of the treaty on 24th December 2014, a milestone that has been widely acclaimed by campaigners and human rights organisations. Sixty-one states have now ratified the treaty, and a total of 130 are signatories.

The most obvious significance of this treaty for human rights law is the requirement at the heart of the treaty for exporting states to make certain assessments relating to the likely consequences of an arms transfer before authorising it to go ahead. This requirement includes a duty to consider the likelihood that the arms in question could be used to commit or facilitate a serious violation of international humanitarian or human rights law. If the exporting State identifies an 'overriding' risk of such consequences, it must not authorise the export. However, before refusing, it must consider whether there are measures that could be undertaken to mitigate the risk, including 'jointly developed programmes' involving the importing and exporting States. This would include programmes aimed at promoting and protecting human rights in the recipient State.

When assessing the likely human rights impact of the proposed transfer, States parties must also take into account the risk that the arms will be used to commit or facilitate serious acts of gender-based violence or violence against women and children. Whilst it is difficult to see what this adds to the above provisions in strict legal terms, it acknowledges the egregious harm that small arms in particular inflict upon women and children, particularly in conflict zones, and the targeting of women and children as a 'military' strategy. In this way the ATT reflects a growing global recognition that violence against women is a distinct and profoundly troubling human rights issue that must be specifically addressed. Ratification and implementation of the ATT has been cited as a desirable measure by CEDAW in its General Recommendation No. 30 on women in conflict prevention, conflict and post-conflict situations.

The ATT's export criteria therefore require States parties to refer back to the existing body of international humanitarian and human rights law when implementing the treaty. However, the provisions are also themselves of interest as far as the development of international human rights law is concerned. The inclusion of human rights as a factor, which in certain circumstances must, at least in theory, override a State's commercial interests, raises questions about the influence of human rights upon public international law in general.

The treaty imposes upon exporting States an international law obligation, albeit one that is limited in scope, in respect of the human rights of individuals in the recipient State. How does this relate to States parties' 'extraterritorial' obligations in international human rights law? Could further international obligations of this type be developed in other contexts? What relationship might this type of provision have to ongoing work on business and human rights, including the UN Guiding Principles on Human Rights? Such issues merit further examination.

There is debate to be had on the extent to which a treaty seeking to regulate rather than circumscribe the global trade in weapons can have a practical positive impact on human rights. Existing humanitarian criteria governing arms transfers in the domestic law of many exporting states have not prevented transfers from proceeding in highly controversial circumstances, and as drafted, the ATT's export provisions leave plenty of space for divergent and self-serving interpretation by States parties. As many commentators have noted, a rigorous approach to implementation, incorporating existing international human rights standards, will therefore be necessary if the ATT is to promote, as a starting point, robust and consistent assessment of the likely human rights impacts of potential arms transfers.

Kate Stone is a barrister at Garden Court North Chambers, Manchester, specialising in human rights law. She is a contributor to the Arms Trade Treaty Legal Response Network (ATT Legal).

"Classic Human Rights Law Territory": Why the HRC Need to Talk About Drones

By Natalie Cargill | 20th October 2014

A US drone strike killed two suspected militants in northwest Pakistan last Saturday, in an attack which marks the seventh this past week, and the sixteenth this year. These latest strikes interrupt a six-month hiatus in drone strikes in Pakistan and follow the first discussion at the Human Rights Council of the use of armed drones. In an unprecedented step, HRC resolution 25/22 called for an expert panel to discuss the use of armed drones, and while some member states objected, there is increasing consensus around the decision to 'officially' consider drone use as a human rights issue.

The panel was held on 22 September 2014 and opened with a series of interventions objecting to HRC as an inappropriate forum to discuss drones. The Council should not – according to the UK delegation – take up weapons "on a thematic basis," or – according to the US delegation – address the "law of armed conflict." Drone use, however, is very much a "Council issue," as was demonstrated in discussions about the legal frameworks applicable to the use of armed drones, the human rights impact of drone strikes and the human rights requirement for transparency and accountability.

The Legal Framework Applicable to Armed Drones

Even in times of armed conflict, a state's international humanitarian law obligations are always complemented by its international human rights law obligations. Flavia Pansieri, Deputy High Commissioner for Human Rights, reflected that "discussions of armed drones have largely focused on the question of whether their use of compatible with the rules and principles of international humanitarian law, which is applicable in situations of active hostilities in the context of an armed conflict. But international human rights law applies at all times, including in situations of armed conflict."

Many legal questions have arisen when a person participates directly in hostilities from the territory of a non-belligerent State, or moves into such territory after taking part in an ongoing armed conflict (such has been the case with Pakistan). The ICRC delegate at the panel noted in this scenario international humanitarian law (IHL) would not be applicable, meaning that such an individual should not be considered a lawful target under IHL, as "advising otherwise would mean that the whole world is potentially a battlefield and that a person moving around the globe could be lawfully targeted under IHL in the territories of States not party to any armed conflict."

The Human Rights Impact of Drone Strikes

Drone strikes have a grave and widespread impact on the lives of individuals and their communities and have compromised the enjoyment of individual rights, including rights to peaceful assembly, education, health, freedom of association and freedom of religion, among others. In addition to loss of life, armed drones create an atmosphere of fear in affected communities, and this fear interrupts education, religious and cultural practices and the enjoyment of basic human rights and fundamental freedoms.

Transparency and Accountability

Both transparency and accountability are key to ensuring that victims of human rights violations can exercise their right to a meaningful remedy. Lack of transparency concerning the circumstances in which armed drones are used, as well as the involvement of intelligence agencies in their use, create obstacles to determining the applicable legal framework and ensuring compliance. As Special Rapporteur, Ben Emmerson, told the HRC, the duty to investigate and transparency are "classic human rights law territory."

As the boundaries of trans-national counter-terrorism operations expand, increased use of remotely piloted aircraft underlines the need for greater consensus on how to apply the international laws that regulate lethal force. Any measures employed to counter terrorism, including the use of remotely piloted aircraft or armed drones, must comply with Charter of the United Nations, international human rights law and international humanitarian law, and respect the principles of precaution, distinction and proportionality. It would seem, then, that more UN involvement is needed, not less.

Natalie Cargill is a University of Oxford graduate and has worked with the United Nations and development NGO's in Geneva. She is currently a GDL student in London.

Iraq Needs Incisive Measures from the UN Security Council

By Michele Porcelluzzi | 30th August 2014

The current US military operations in Northern Iraq, resisting troops belonging to the Islamic State of Iraq and Syria (ISIS), may be evaluated as compatible with international law. However, despite this, UN Security Council measures are still needed.

According to Article 2 (4) of the UN Charter and customary international law, the use of force is legal only in cases of self-defense, or on the authorization of the Security Council acting under Chapter VII, with respect to threats to peace, breaches of the peace, and acts of aggression.

In recent weeks, ISIS troops have attacked cities in the North of Iraq, committing gross violations of human rights. In order to repel them, the US is currently carrying out targeted military operations. These have a dual aim: to protect American people and facilities inside of Iraq and to help save thousands of Iraqi civilians, such as those besieged on Mount Sinjar. Further, the EU is providing military support to beleaguered Kurds in northern Iraq.

In a letter issued on August 8, President Obama justified these military operations to Congress as "necessary to protect American personnel in Iraq by stopping the current advance on Erbil by [ISIS]." However, the existence of the right to use force in order to protect nationals is undoubtedly controversial.

Further, the military operations in north Iraq are not classifiable as "humanitarian intervention." Typically, a humanitarian intervention, like that in Kosovo in 1999, is conducted by a State or a group of States against another State, which is committing gross violations of its citizens' human rights. At present, the legality of a "humanitarian intervention" is one of the most controversial issues in international law. In this case, ISIS – and not the Republic of Iraq – is committing atrocities against Iraqi citizens. Therefore, this cannot a "humanitarian intervention" as currently understood.

The self-defense argument is the most persuasive. ISIS is attacking a sovereign State, the Republic of Iraq. According to article 51 of the UN Charter, the State has an inherent right of individual or collective self defense. In compliance with international customary law, there are three requirements that have to be satisfied: first, there must be an actual or imminent armed attack against a State; second, the attack must attain a minimum scale; finally, the armed response must be necessary and proportionate. In this case, the US military operations in Iraqi territory have been authorized by the local government in order to combat the illegal aggression of ISIS and to prevent gross violations of human rights. It is therefore clearly a case of collective self defense allowed by the UN Charter, though the use of force must, of course, be both proportionate to repel the attack and not excessive.

On August 15, the UN Security Council adopted Resolution 2170 (2014), which condemned "gross, systematic and widespread abuse" of human rights by ISIS and Al-Nusra Front. Further, it called on Member States to take national measures to prevent fighters from travelling from their territories to join the groups, and it named individuals related to ISIS who would be subject to travel restrictions, asset freezes and other measures targeted at Al-Qaida affiliates.

However, this Resolution appears insufficient to stop the attacks of ISIS, as it establishes sanctions only for six individuals and does not authorize the use of force. In contrast, the US military intervention is incisive – as a result of this intervention, Iraqi troops have retaken Mosul dam from ISIS militants – but unilateral. It is only the United States that decides when and where bombarding occurs, with no plan agreed with any other State or International Organizations.

Iraq now needs incisive and multilateral measures, established by the UN, capable of stopping ISIS. The lives of thousands of Iraqi citizens are at risk. Can the world stand by and watch?

Michele M. Porcelluzzi completed his M.Sc. in Law at Bocconi University in 2010. His research interests include International Public Law, International Humanitarian Law, Human Rights Law and National Security Law.

Dignifying the Most Vulnerable 'In' and 'Through' Security Council Resolution 2139

By Sarah M. Field | 19th March 2014

Conflict – perhaps more than anything else – illuminates our shared vulnerability to hurt and harm of unimaginable form and depth. The legal protection of rights was born of such suffered injustice, as articulated in the UN Charter. To an extent then, it may be viewed as juristic response to our embodied vulnerability. Therein lies one of the enduring paradoxes of international human rights law; the most vulnerable frequently have the least access to justice.

Consider the hundreds of thousands besieged in Syria: over a thousand days since the conflict began, rights violations cascade--violations of the rights to life, freedom from hunger and of movement layer upon violations of the rights to legal remedies, to take part in public affairs and the rights to freedom of expression and association, amongst others. And, the sole possibility of redress is conditional on one of the most precarious of all political processes – decision-making towards peace agreements.

Geneva II presented hope. The Communiqués of Geneva I and the London 11 both required ensuring the right to humanitarian assistance as a part of more substantive negotiations. As the two-staged process stalled to a fracturing halt on the 15th February, hope transferred to the Security Council. The decision to adopt Resolution 2139 – *demanding* the parties to the conflict respect and ensure respect for applicable international law – presented a breakthrough. However, the imperative for the resolution, the process of its adoption and the substance of the resolution, including the missing (negotiated-out) provisions, illuminates, under harsh light, the inadequacies of international law. Of course, the multifarious instruments of international human rights and humanitarian law include vital – dignity affirming – devices. If the Syrian State had implemented the past recommendations of the Human Rights Committee, might the conflict have been averted? And if the parties to the conflict had heeded the guidance of the guardian of international humanitarian law, might the hurt and harm have been lessened? Of course, the operative word here is – *if*.

The international community steps into the breach 'in' and 'through' the Charter bodies. For the people living under siege, these are also vital spaces for their rights to be seized, shaped and expressed. General and Syria-specific recommendations and decisions

provide a basis for advocacy and redress now and into the future, including, for example, the decision by the Human Rights Council to establish an Independent International Commission of Inquiry.

However, the form and process of decision-making (including rules) also may be viewed as concurrently creating vulnerability in the form of exclusion. For example, whereas the Syrian State was represented within the Security Council, those made vulnerable by the *forces* of the State were unrepresented; they were *dependent* on the international community seizing, shaping and expressing their rights. This is also a process by (in)action: whether or not their rights are secured is *dependent* on political agreement about the facts and the response – specifically among the five veto-wielding members.

The vulnerability effects of the latter are obvious and graphically illustrated by the resolution: the *demands* on the parties to the conflict to respect and ensure respect for international law are not matched by *decisions* to secure the right to humanitarian assistance of the people of Syria. However the form and process also create vulnerability in a more subtle way by subverting the position of the right-holder – reframing bearers of rights to objects of international protection. De jure, the people under siege remain 'equal in dignity and rights.' De facto (without representation and effective remedies), they are dependent on a precarious collision of legal, political and principled imperatives for redress. Viewed in this way, neither the process nor the outcomes dignify the people of Syria.

Though deeply inadequate, the resolution is nonetheless a vital dignity-affirming agreement. First, it states that international law matters, rights matter. Second, it illumines the potentialities of law into the future, connecting violations to international crimes, establishing a monitoring and reporting mechanism and expressing an intention for further action upon non-compliance. Third, it re-affirms the import of a rights-based political solution: the full participation of the people of Syria 'in' and 'through' the peace trajectory. Countering the inaction, then, is the fact of agreement by a divided Security Council. Geneva II stalled; the right to veto looms over future Security Council decisions with foreboding bleakness; the question of how to secure the rights of the most vulnerable remains – reducing us all.

Sarah M. Field is a Human Rights Practitioner with global experience supporting the rights-based development of the rule of law, a Post-Doctoral Researcher at the Faculty of Law, University College Cork, Ireland and the founder of a developing legal advocacy project asking the child question.


UN