

Open-Source Intelligence, Armed Conflict, and the Rights to Privacy and Data Protection

Threats and Conceptual Challenges

Edward Millett

Edward is an English-qualified lawyer and legal researcher.

This article is based on thesis research conducted by the author at the Geneva Academy of International Humanitarian Law and Human Rights under the supervision of Professor **Gloria Gaggioli**.

DOI: [10.58866/HQKE7327](https://doi.org/10.58866/HQKE7327)

Abstract

This paper examines the use of open-source intelligence (OSINT) during armed conflict and in humanitarian-emergency settings by States and non-State actors. It highlights real-world harms that can arise from the misuse of OSINT in such contexts, in particular through the lens of the rights to privacy and data protection, thereby demonstrating gaps in current terminology, regulatory frameworks, and ethical practices governing the use of this technology.

Regarding OSINT's use by States, the paper highlights the limits of existing legal frameworks regulating digital privacy and data protection in conflict settings, drawing on domestic regulatory frameworks and parallels from human rights law to identify key conceptual problems and regulatory limitations. Where non-State actors use OSINT, this paper highlights – via two case-study users, Bellingcat and the OSCE's Special Monitoring Mission in Ukraine – the 'doctrinal gap' that arises from the patchwork of ethical standards and the relative absence of legal restraints. This gap poses a risk of harm to individuals and communities affected by OSINT activities that needs to be rectified, initially through the development of an evidence-based 'theory of harm'.

Keywords

open-source intelligence – OSINT – privacy – data protection – armed conflict – international humanitarian law – international human rights law – social media – OSCE – Bellingcat – investigatory powers

Introduction

Open-source intelligence (OSINT) – publicly-available information that has been discovered, analysed, and disseminated¹ – is becoming a constant feature of armed conflict in the 21st century. In the context of the Russia-Ukraine conflict alone, private-sector satellite companies are providing geospatial data to the Ukrainian military,² civil-society organisations are using geolocated footage and social media posts to map incidents of civilian harm,³ and international organisations have previously used drones to monitor ceasefire compliance.⁴ Widespread use of such OSINT tools and techniques to acquire, analyse and disseminate information, undertaken by a range of actors, is therefore engendering a 'foundational shift' away from States' role as the 'ultimate arbiters' of public access to intelligence during armed conflict.⁵

This shift is revealing significant positive opportunities, with OSINT supporting efforts to fight disinformation and uncover human rights abuses,⁶ to refine military targeting,⁷ to monitor

1 Heather Williams, Ilana Blum, 'Defining Second Generation Open Source Intelligence (OSINT) for the Defence Enterprise', *RAND Corporation* (2018) p. 8.

2 Mike Cerre, Dan Sagalyn, 'Private companies track the war in Ukraine in real time' *PBS Newshour* (2022).

3 Bellingcat Investigation Team, 'Hospitals Bombed and Apartments Destroyed: Mapping Incidents of Civilian Harm in Ukraine', *Bellingcat* (2022).

4 Cono Giardullo, A. Walter Dorn, Danielle Stodilka, 'Technological Innovation in the OSCE: The Special Monitoring Mission in Ukraine' in IFSH (ed.) *OSCE Yearbook 2019* (2020) p. 120.

5 Ardi Janjeva, Alexander Harris and Joe Byrne, 'The Future of Open Source Intelligence for UK National Security', *RUSI Occasional Paper* (2022) p. 11.

6 John Thornhill, 'Ordinary Ukrainians wage war with digital tools and drones', *Financial Times* (2022).

7 Asaf Lubin, 'The Rights to privacy and data protection under international humanitarian law and human rights law' in Robert Kolb, Gloria Gaggioli, Pavle Kilibarda (eds.), *Research Handbook on Human Rights and Humanitarian Law* (2022) p. 487.

ceasefires,⁸ and to gather criminal evidence.⁹ However, there are also significant threats posed by the acquisition, analysis, retention, and dissemination of publicly-available information. A couple of examples: by revealing to the Taliban valuable personal information about Afghan citizens collaborating with NATO-coalition partners through website and social media posts;¹⁰ by accidentally divulging the location of demobilised child soldiers through the piecing together of disparate, public information sources (the ‘Mosaic effect’);¹¹ by encouraging an unregulated online hunt for a suspected criminal fugitive through the publishing (‘doxxing’) of their personal information;¹² or by accidentally alerting the authorities to the existence of an undocumented crossing in ceasefire lines through drone footage production, resulting in curtailment of civilian access, via the crossing, to schools, workplaces, and community services.¹³ The above examples sketch out some of the threats to individuals and communities posed by the use of OSINT by various actors, States, and others. What unites these examples is an insufficient appreciation for the real-world impacts, direct and indirect, posed by the acquisition, analysis, retention, and dissemination of publicly available information.

Accordingly, this paper will consider threats and conceptual challenges associated with the use of OSINT during armed conflict and in humanitarian settings, with a particular focus on fundamental privacy and data protection rights. It will seek to show that current legal and ethical frameworks restraining the use of such techniques are not sufficiently modernised or harmonised. Moreover, the lack of clear definitions of terminology and of underlying notions regarding what information is ‘publicly available’, is clouding a better understanding of applicable norms and possible harms arising from the use of OSINT, particularly regarding privacy and personal data protection. This definitional problem tracks across into States’ understanding of their legal obligations under applicable international humanitarian law (IHL) and international human rights law (IHRL) with regard to the use of OSINT. Below, an analysis of the surveillance authorisation framework in the UK will serve as an example of how contemporary privacy frameworks are struggling to bring State-led OSINT activities fully within the scope of existing rules.

For non-State OSINT activity, the relative absence of legal restraints requires a closer look at current practice and their own understanding of ethical and operational restraints. Through examination of two case studies – a civil-society organisation (Bellingcat) and an international organisation (OSCE) – this paper highlights the patchwork of varied ethical standards that has developed, resulting in a ‘doctrinal gap’, posing a risk of harm to individuals and communities.¹⁴ A crucial precursor to rectifying this will be the development of an evidence-based ‘shared theory of harm’ that is specific to the negative impacts of such technological applications as OSINT in armed conflict settings by such user groups.¹⁵

8 Giardullo *et.al. supra* n. 4.

9 Lindsay Freeman, ‘Prosecuting Atrocity Crimes with Open Source Evidence: Lessons from the International Criminal Court’, in Sam Dubberley, Alexa Koenig, Daragh Murray (eds.) *Digital Witness* (2019) pp. 68-86.

10 Based on Amanda Connolly, ‘Global Affairs Canada is purging websites, social media amid Taliban takeover’, *Global News* (2021).

11 Nathaniel Raymond, ‘Beyond “Do No Harm” and Individual Consent: Reckoning with the Emerging Ethical Challenges of Civil Society’s Use of Data’, in Linnet Taylor, Luciano Floridi, Bart van der Sloot (eds.) *Group Privacy: new challenges of data technologies* (2017) p. 95.

12 Interview with Bellingcat staff member, 4 August 2022

13 Interview with former member OSCE Special Monitoring Mission to Ukraine, 30 July 2022

14 Raymond *supra* n. 124 p. 85.

15 Kristin Sandvik, Nathaniel Raymond, ‘Beyond the Protective Effect: Towards a Theory of Harm for Information Communication Technologies in Mass Atrocity Response’, *Genocide Studies and Prevention* Vol.11 Iss.1 (2017) p. 16.

Structure

Part I will consider prevailing definitions of OSINT (and related terms) across various user groups, spotlighting a number of key issues that arise from the lack of an accepted, unified definition. Part II will then explore how the use of OSINT by States in armed conflict settings can be regulated by IHL and IHRL, identifying conceptual issues and issues of legal application. By way of example, a closer consideration of the domestic surveillance authorisation regime in the United Kingdom serves to highlight how ongoing uncertainties around the definition and scope of OSINT pose a challenge to situating such activities within existing privacy regulation frameworks. Part III will then explore how far the use of OSINT by non-State actors is restrained by current legal and ethical frameworks, spotlighting Bellingcat and the OSCE's use of OSINT. Finally, Part IV will flag up other 'threat vectors' alongside privacy/data protection concerns, particularly relating to the use of demographically identifiable information and the challenges with obtaining informed consent from the data subject.¹⁶

Part I - Defining open-source intelligence

Open-source intelligence (OSINT) is a 'dynamic term that often consists of contradictory or ambiguous pre-requisites', meaning that a single unified definition does not currently exist, either operationally or legally.¹⁷ Similarly, there are currently no unified definitions of related terminology such as 'open-source information' (OSIF), 'open-source investigations', or 'open-source operations'. However, users are generally in agreement on the distinction between OSIF and OSINT: turning open-source *information* into open-source *intelligence* requires that it be 'discovered, discriminated, distilled, and disseminated to a select audience'.¹⁸ This is of crucial importance to defining the scope of OSINT *operations*, which go beyond simple data-collection to include the full information 'operations cycle' of data processing, exploitation, and (re)production.¹⁹ This reality has ramifications for any analysis of the risks to privacy/data protection posed by OSINT, since activities comprise data *acquisition* – posing a threat to the confidentiality of data; *retention* – which may impose data protection obligations on the retaining party; and *publication* – likely to have privacy ramifications for individuals.²⁰ Geiß and Lahmann have usefully highlighted three core 'data security' concepts that provide analytical clarity on the impact of OSINT operations.²¹ "Data confidentiality" relates to protecting data from unauthorised access and is 'closely related to and a precondition of privacy'.²² OSINT operations are most likely to threaten this aspect of data security by obtaining access to personal information that has found its way into the public domain. "Data integrity" refers to 'maintaining and assuring...the accuracy and completeness of stored data', which indicates the fundamental nature of data protection standards such as accuracy and security.²³ "Data availability" relates to data being 'accessible and...processable' when required.

16 Raymond, *supra* n. 124 p. 84.

17 Douglas Wells, Helen Gibson, 'OSINT from a UK perspective: considerations from the law enforcement and military domains' *Proceedings Estonian Academy of Security Sciences* 16 (2017) p. 86.

18 NATO, 'Open-source Intelligence Handbook' (2002) pp. 2-3.

19 Williams/Blum *supra* n. 1 p. 13; c.f. Isabelle Böhm, Samuel Lolagar, 'Open source intelligence: Introduction, legal and ethical considerations' *International Cybersecurity Law Review* 2 (2021) pp. 320-1.

20 Robin Geiß, Henning Lahmann, 'Protection of Data in Armed Conflict', 97 *International Law Studies* 556 (2021) p. 562.

21 Geiß/Lahmann *supra* n. 20 pp.561-2

22 *Ibid.*

23 E.g. GDPR Art.5(1)(d),(f).

Nevertheless, there remains fundamental divergence in the understanding of what is truly ‘open-source’. I suggest that this is for two broad reasons. First, the diverse range of different users of open-source – including State intelligence and military actors, international courts, and human rights groups – with differing operational priorities, legal constraints, approaches, and reputational considerations. Second, there remains a divergence between user groups over (i) what information is deemed *publicly available* and (ii) what *means* of collection – overt or covert – are appropriate to gather that information.

Divergence between user-groups

Numerous attempts at a definition of OSINT/OSIF and related concepts exist in the realm of intelligence and law enforcement. For example, the US Office of the Director of National Intelligence (ODNI) in 2011 suggested that OSIF is ‘information that any member of the public can observe, purchase or request, without requiring special legal status or unauthorised access’.²⁴ This would include mass media, specialised journals, conference proceedings and think-tank studies, photography, and geospatial information, including digital maps and commercial satellite imagery. Similarly, the UK National Police Chiefs’ Council’s (NPCC) working definition of OSINT requires that information must be derived from ‘publicly-available information’: information that any member of the public could *lawfully* obtain by request or observation, *including for payment*.²⁵ Accordingly, this brings commercial data sources – shipping data, databases, satellite imagery services – into scope, as well as information obtained through legal mechanisms such as freedom-of-information requests.

Civil-society organisations would disagree on elements of this definition, given their distinct operational priorities, reputation, and outlook. For example, a view is now emerging amongst civil-society users that whereas data services provided for a ‘nominal fee’ can be considered open-source, commercial subscription services – which can cost hundreds or thousands of dollars monthly cannot – on the basis that the financial barriers to entry are too high.²⁶ Similarly, regarding the legality and ethics of open-source activities, the Berkeley Protocol – a leading soft-law framework for open-source investigations aimed at civil-society users – calls on investigators to respect the right to privacy, but only on the limited basis that violations may result in evidence being excluded from criminal proceedings.²⁷ Finally, more prosaic concerns factor into the divergence of terms and definitions for open-source activity: for example, Bellingcat, an investigatory NGO, shuns the term open-source ‘intelligence’ altogether, given the perceived implication that open-source information is being validated with secret intelligence provided by Western intelligence agencies – an allegation repeatedly levelled at the organisation by hostile State actors.²⁸

Open-source information gathering: what can be collected and how?

The second key reason for the divergence in the definition of OSINT and related terms arises from disagreement over what information is *publicly available* and what *means* of collection – overt or covert

24 Office of the Director of National Intelligence, ‘Civil Liberties and Privacy Guidance for Intelligence Community Professionals’ DNI Pre-Pub 20140708 (2011); Human Rights Center, UC Berkeley School of Law and the Office of the High Commissioner for Human Rights, *Berkeley Protocol on Digital Open Source Investigations* (2020) p. 3.

25 National Police Chiefs’ Council, ‘NPCC Guidance on Open Source Investigation/Research’ (2015) [Redacted] p. 4.

26 Geneva Academy of International Humanitarian Law and Human Rights, ‘Open-source information: strengthening accountability at the intersection of law, technology and the humanitarian space’, Open-source information Conference, Geneva, 14 December 2022.

27 Berkeley Protocol *supra* n. 24 para. 62.

28 Interview with Bellingcat staff member, 4 August 2022

– are appropriate to gather that information. This is inherently connected with the nature of the user: for example, a State and an individual conducting open-source research may have different perspectives on what paid services are in-scope and what the nature of their legal, ethical, and reputational obligations and motivations are.

One of the key issues in determining the scope of OSINT activities remains the question of what is ‘publicly available’, which is central to an analysis of how OSINT interacts with the human right to privacy. A traditional view holds that whatever information is shared online is public, publicly accessible, and remains the responsibility of the individual sharing it.²⁹ However, this position is becoming increasingly contested, given the scope and sophistication of information gathered from social media websites (SOCMINT) of detailed personal data.³⁰ For example, a public post by a Facebook user with an open profile (i.e., unrestricted privacy settings) would be widely considered publicly available, but there is much more uncertainty about the public nature of, for example, their posts in a 30-person community group, or the ‘social graph’ of their friends on the platform, or in situations where a researcher adopts a fake persona to obtain access to the target’s profile.³¹ Janjeva et al. have taken a more blanket approach, considering that where a user-verification requirement is in place to access a platform – a pre-requisite of Facebook access – SOCMINT can no longer be considered publicly available.³²

In terms of what type of information can be considered open-source, a key part of this dispute concerns the acquisition, analysis, and reproduction of information that has been hacked, leaked, exposed by security vulnerabilities, or posted by a third party without authorisation. Such information would likely fall outside the ODNI and NPCC definitions, implying a need for legal authorisation to acquire. The Berkeley Protocol, however, considers this information ‘technically’ open-source while cautioning legal and ethical restrictions on its use.³³ More broadly, amongst civil-society actors, there appears to be variance in appreciation and prioritisation of these restrictions with respect to leaked material.³⁴

The other consideration is the extent to which information gathered *covertly* may be considered open-source. For example, a definition of OSINT proposed by the CIA in 2010 clearly discounts covert collection techniques from the scope of open-source information-gathering.³⁵ By contrast, the NPCC’s framework for the use of open-source information in UK law-enforcement operations considers that covert operations to gather such information would still constitute open-source investigation – although obtaining surveillance authorisation *may* still be appropriate.³⁶ In this context, Edwards and Urquhart have proposed a useful typology for considering whether data acquisition from social media sites is overt or covert. They distinguish ‘open’ information from ‘closed’ information – the latter ‘restricted by Friends locks, passwords, encryption, etc.’³⁷ Further, they distinguish ‘overt’ from ‘covert’ tactics, where data

29 Alexander Gillespie, ‘Regulation of Internet Surveillance’ 4 *EHRLR* (2009) p. 552.

30 Böhm/Lolagar *supra* n.19 pp. 320-1.

31 Lilian Edwards, Lachlan Urquhart, ‘Privacy in public spaces: what expectations of privacy do we have in social media intelligence?’ *International Journal of Law and Information Technology* 24 (2016) p. 295.

32 Janjeva et.al. *supra* n. 5 p. 5.

33 Berkeley Protocol *supra* n. 24, p. 6.

34 Geneva Academy OSINT Conference, *supra* n. 26.

35 Wells, Gibson *supra* n. 17 p. 86.

36 NPCC *supra* n. 25 p. 9.

37 Edwards/Urquhart *supra* n. 31 pp. 291-2.

subjects are not fully aware and informed or are deceived or misled as to the nature, extent, and purposes of the access or processing of personal data. ‘Covert’ data acquisition may include: befriending someone with an anonymous profile, gaining access to private groups, or ‘leveraging’ certain responses by posting provocative content.³⁸ By contrast, the Berkeley Protocol adopts a more blanket attitude to covert, unauthorised methods of acquiring information: simply put, acquiring such information ‘does not involve interacting with or soliciting information from individual Internet users’.³⁹

The discussion above makes clear that the definitions of terms such as OSIF and OSINT adopted by users are diverse, changing over time, and reveal differences in the understanding of issues such as individual privacy in the digital environment and users’ responsibilities thereto – all of which makes reaching a common set of definitions that is acceptable to all users difficult. In the following section, we will see how the lack of common definitions impacts the approach taken by States to their privacy and data protection responsibilities, but more broadly, it is clear that the absence of commonly understood terminology is fuelling uncertainty about the prevailing norms and possible harms that attach to open-source activities in general.

Part II - OSINT and Privacy: States

Turning to the threats posed by the use of OSINT techniques by States during situations of armed conflict, privacy, and data protection rights stand out prominently. OSINT activities by States can take the form of ‘directed surveillance’ against individuals, including via both covert and overt approaches to gathering, analysing, and publishing personal information online. In armed conflict settings, OSINT activities can be situated within the wider remit of cyber operations, although, unlike other cyber operations, they are not usually aimed at the loss of functionality within computing systems.⁴⁰ Nevertheless, OSINT activities potentially interfere with rights preserved by IHL and IHRL. This section, therefore, assesses the extent to which IHL regulates State OSINT operations against personal data, then considers how IHRL can gap-fill.

OSINT and Privacy under IHL

Wartime informational privacy, i.e., the concurrent application of digital rights during armed conflict, remains something of a lacuna in contemporary IHL.⁴¹ Nevertheless, the rights to privacy and data protection stem from the same foundational value as a key tenet of IHL: the protection of human dignity.⁴² Prisoners of war and protected civilians are already shielded from exposure to ‘public curiosity’ by the Geneva Conventions in international armed conflict, a prohibition that may incorporate both obtaining and disseminating images or private data of such persons.⁴³ This suggests that OSINT activities directed against the personal data of such persons could violate IHL both in terms of data acquisition and data publication. These treaty provisions, therefore, provide a starting point for considering how far activities across the whole open-source operations cycle (collection, processing,

38 *Ibid.*

39 Berkeley Protocol *supra* n. 24, p. 7.

40 Heather Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 *Israel Law Review* 1 (2015) pp. 39,42.

41 Lubin *supra* n. 7 p. 477.

42 ICRC ‘The Fundamental Principles of the International Red Cross and Red Crescent Movement’ p. 3.

43 Art.13 GCIII; Art.27 GCIV; ICRC, *Commentary on the Third Geneva Convention* (2020) §1624.

exploitation, and (re)production) are regulated by IHL at present.⁴⁴

Medical Data

The Tallinn Manual 2.0, a non-binding instrument, has significantly developed the understanding of international law applicable to cyber operations in armed conflict. While the Manual is largely focused on cyber-targeting rather than the status of fundamental digital rights, it identifies medical data as a particular protected data type. Personal medical data enjoys *some* particular protections in the context of cyber operations. Patient records or other information relating to individuals in treatment, as well as any other data “belonging to medical units and their personnel” are considered within the scope of the medical services and infrastructure that conflict parties are obligated to “respect and protect”.⁴⁵ The scope of this obligation is wide. The Tallinn Manual states:

“Personal medical data required for the treatment of patients is...protected from alteration, deletion, or any other act by cyber means that would negatively affect their care, regardless of whether the act amounts to a cyber attack.”⁴⁶

The implication of this is that OSINT activities, when undertaken by a conflict party, need not amount to a ‘cyber-attack’ to engage the State’s IHL obligations: it is sufficient that the activity is ‘any other act by cyber means’ (such as data-acquisition, retention or publication) that would negatively affect patient care.⁴⁷ This is a significant development where, for example, OSINT activities are used to gain access to personal medical data of *hors de combat* service personnel and civilians. It also highlights the ‘privacy paradox’—just because such data is publicly available does not mean it is not protected.⁴⁸ Further, it suggests that cyber operations targeting data confidentiality, integrity, or availability may still be prohibited by IHL, even in cases where they do not directly harm the computer system or patients.⁴⁹ Some scholars have proposed expanding the scope of IHL’s protections for medical data. O’Connell argues that the same logic that justifies extending protection under IHL to aspects of medical care that are not expressly mentioned in IHL treaties can be used to extend protections from medical data to other personal data.⁵⁰ There are, however, convincing arguments *against* such an interpretation, as O’Connell acknowledges: the specific mention of ‘medical’ infrastructure in treaty provisions would exclude non-medical infrastructure from protection, while it does not necessarily follow that the most protective interpretation of a provision of IHL is always the correct one.⁵¹

Non-medical Personal Data

If medical data is conceived of as a sub-category of personal data benefiting from specific protections,

44 Williams/Blum *supra* n. 1 p. 13.

45 Geiß/Lahmann *supra* n. 20 p. 564; Michael Schmitt (ed.), *Tallinn Manual 2.0* (2017) Rule 132; ICRC, *Customary IHL Database*, Rules 25,28,29.

46 Schmitt *supra* n.45 Rule 132§3 [emphasis added].

47 ‘Cyber-attack’ is defined in the Tallinn Manual as ‘a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.’ (Rule 30).

48 Leonore Ten Hulsen, ‘Open Sourcing From The Internet – The Protection Of Privacy In Civilian Criminal Investigations Using OSINT (Open-Source Intelligence)’ (2020) 12 *Amsterdam Law Forum* Vol.1 p. 36.

49 Geiß/Lahmann *supra* n. 20 p. 563.

50 Mary Ellen O’Connell, ‘Data Privacy Rights: The Same in War and Peace’ in Russell Buchan, Asaf Lubin (eds.) *The Rights to Privacy and Data Protection in Times of Armed Conflict* (2022) pp. 24-5.

51 *Ibid.* p. 25.

the impact of OSINT operations on personal data *more broadly* poses greater conceptual problems. This is connected with the ongoing debate as to whether digital data, in general, is eligible to fall within the protections of IHL's targeting rules on distinction, proportionality, and precautions.⁵² Geiß and Lahmann have argued, based on a contextual-teleological reading of Art.52 API, that personal data is protected from being made the 'object of attack' unless converted to a military object.⁵³ However, for OSINT activities, the key uncertainty at present is whether an OSINT cyber-operation qualifies as an 'attack' within the Art.49 API definition, thereby rendering the protections of IHL applicable to personal data. Schmitt has suggested that operations aimed at affecting the *integrity* of data – to use Geiß and Lahmann's formulation described earlier – would qualify as an 'attack', whereas operations that leave data intact and only target *confidentiality* would not.⁵⁴ However, it follows from this that the full OSINT operations cycle of data collection, processing, exploitation, and (re)production could be effectively conducted by combatants to gather, analyse and republish personal information without affecting data integrity, thereby falling outside IHL's protection entirely. This conclusion leaves OSINT operations against non-medical personal data in a lacuna under IHL.

One solution has been proposed by Watt: expanding the scope of Art.57 API's duty of 'constant care', part of the mandatory precautions in attack, to include taking care to avoid the deleterious effects of cyber operations on civilians where a nexus exists between the data-based activity and the advancement of combat goals.⁵⁵ The Tallinn Manual indicates that the commander's duty to respect the civilian population extends to cyber operations;⁵⁶ it follows that this duty could be expanded to periods prior to the conflict and to a wider range of informational activity – including the collection, processing, storage, and dissemination of data – in order to 'operationalise the duty of constant care in the digital age'.⁵⁷ The implication of this interpretation of the 'constant care' duty would be to import privacy and data protection principles from IHRL wholesale within the remit of IHL.

OSINT and Privacy under IHRL

While stakeholders such as the International Committee of the Red Cross (ICRC) have highlighted the role that IHRL can play in substantiating regulations on surveillance and disinformation generally in wartime, for now, a holistic framework does not exist.⁵⁸ A limited example of IHRL's emerging role in regulating privacy in armed conflict can already be seen in the ICRC's commentary to the Second Geneva Convention, which notes that personal health data held by hospital ships 'must be afforded a reasonable level of security' in accordance with 'international privacy and data protection standards'.⁵⁹ Accordingly, to highlight the current conceptual and legal limitations on the regulation of OSINT operations during armed conflict, the following section will survey IHRL privacy and data protection norms applicable to OSINT operations *in peacetime* before considering how these can be 'read across to armed conflict

52 Schmitt *supra* n. 45 p. 437.

53 Geiß/Lahmann *supra* n. 20 p. 566-7.

54 Michael Schmitt, 'The Notion of "Objects" During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision', 48 *Israel Law Review* 81, (2015) pp. 95,101.

55 Eliza Watt, 'The Principle of Constant Care, Prolonged Drone Surveillance and the Right to Privacy of Non-Combatants in Armed Conflicts' in Russell Buchan, Asaf Lubin (eds.) *The Rights to Privacy and Data Protection in Times of Armed Conflict* (2022) p. 175.

56 Schmitt *supra* n. 45 p. 477.

57 Lubin *supra* n. 7 p. 8.

58 ICRC, 'IHL and the Challenges of Contemporary Armed Conflicts' (2019) p. 21.

59 ICRC, *Commentary on the Second Geneva Convention* (2017) §2403.

settings.⁶⁰ The regulatory framework for the surveillance authorisation system in the United Kingdom will serve as an illustrative case study; a more holistic multi-jurisdictional analysis is outside the scope of this paper, although a valuable next step for research in this field.

When does OSINT infringe upon privacy rights?

Applying privacy and data protection standards under IHRL to State OSINT operations in a domestic setting poses significant conceptual issues. The primary issue concerns the question of whether collection, storage, retention, use, and dissemination of private material without individual consent from public digital spaces, such as social media websites, infringes upon the right to privacy. As a starting point, the European human rights system has endorsed the idea of ‘privacy in public’, albeit usually in relation to cases where private material was *disseminated*, not simply *accessed*. The leading case remains *von Hannover v Germany*, where the European Court of Human Rights (ECtHR) held that the publication of photos of the Princess of Monaco fell within the ambit of her right to private life.⁶¹

It is, however, less clear whether privacy rights would be infringed where private material disclosed in public is acquired, retained, and processed – all key aspects of the OSINT operations cycle along with publication. In *Rotaru v Romania*, the ECtHR, in finding a violation of Art.8 of the European Convention on Human Rights (ECHR), held that ‘public information can fall within the scope of private life where it is *systematically collected and stored* in files held by the authorities.’⁶² This view has been reinforced in *Segerstedt-Wiberg v Sweden*, a case concerning files kept by security police drawn from open sources such as print media. The ECtHR held that even publicly-obtained parts of the file pertained to the applicant’s privacy since ‘the information has been *systematically collected and stored* in files held by the authorities.’⁶³ Edwards and Urquhart, therefore, conclude that the current state of ECtHR jurisprudence entails that publicly-available SOCMINT concerning private life can be lawfully observed and collected so long as it is not turned into a ‘detailed dossier on a particular data subject.’⁶⁴ In computer-science terms, they characterise the distinction drawn by jurisprudence as being between the gathering of ‘structured data’ – which can be queried and data-mined – and ‘unstructured’ data – which cannot.⁶⁵ However, their view is that this distinction is no longer fit for purpose: as the European Court of Justice acknowledged in *Google Spain* (the ‘right-to-be-forgotten’ case), nowadays, ‘any internet user’ can use a search engine to obtain a ‘structured overview’ of information on an individual, and thereby ‘establish a...detailed profile of him’.⁶⁶ The ramifications of this are significant, highlighting that even fairly basic OSINT activities online may constitute an interference with individual privacy rights. Accordingly, even cases of overt acquisition of freely-accessible information on a data subject could fall within the ambit of privacy law, entailing a need for surveillance authorisation.

60 Art.17 ICCPR prohibits arbitrary or unlawful interferences with an individual’s privacy. The right is also articulated, inter alia, in ECHR Art.8, IACHR Art.11, and the EU Charter Art.7. While the AfCHPR lacks a formal right, one can be located in the African Declaration on Freedom of Expression and Access to Information 2019 (Principle 40). See Yohannes Ayalew, ‘Untrodden paths towards the right to privacy in the digital era under African human rights law’, *International Data Privacy Law*, Vol.12, Iss.1, pp. 20-1. The HRCtee has confirmed that the right to privacy extends to informational privacy such as online communications. See UN HRCtee, *General Comment No. 16* (1988) §10. The notion of freestanding data protection rights has emerged more slowly and includes the Council of Europe’s Convention 108+, the EU Charter, the African Union’s Malabo Convention, and GDPR.

61 *von Hannover v Germany* [2005] 40 EHRR 1.

62 *Rotaru v Romania* [2000] 8 EHRC 449 §43 [emphasis added].

63 *Segerstedt-Wiberg v Sweden* [2007] 44 EHRR 2 §72.

64 Edwards/Urquhart *supra* n. 38 p. 307.

65 *Ibid.*

66 *Google Spain v Costeja González*, ECJ, Case C-131/12 [2014] §80.

Obtaining surveillance authorisation - the UK system

Where a State's OSINT activities *do* infringe on privacy rights, it must obtain domestic legal authorisation in order to uphold the principles of legality, necessity, and proportionality. An overview of the domestic surveillance authorisation framework in the UK serves to illustrate the conceptual complexities of positioning OSINT within such frameworks. In the UK, legal authorisation for the police and intelligence services to surveil an individual online is primarily provided under the Regulation of Investigatory Powers Act 2000 (RIPA).⁶⁷ As a minimum, authorisation under RIPA to undertake directed, 'covert' surveillance would entail obtaining a Directed Surveillance Authority (DSA).⁶⁸ As discussed, delineating which OSINT activities are 'covert' and which are not is complex: government policy guidance indicates that the relevant standard for assessing whether a DSA is required is the 'reasonable expectation of privacy.'⁶⁹

This raises two key issues. First, as highlighted above, the uncertainty regarding whether OSINT activity is actually covert or overt. For the purposes of the *statutory* definition in RIPA, simply viewing a Facebook user's open profile is considered 'covert', thus entailing the requirement to obtain a DSA.⁷⁰ A rich range of data types can be mined from a Facebook user's public profile without their knowledge, including such as the 'social graph' of a person's friend network – a valuable data source that has historically been hard to hide from public exposure – or posts about that person by other users.⁷¹

Second, delineating what information falls within the scope of a 'reasonable expectation of privacy' is very difficult to establish with clarity and may vary across different sections of a social-media platform and user age groups.⁷² A Facebook user may have a higher expectation of privacy in a private 30-person community group than in respect of their public posts. De George has also suggested that people have a misguided intuition of privacy when they act online since they often do so 'in the privacy of their homes', neglecting the fact that the 'transaction does not take place in the physical space they delimit as private.'⁷³ It can be difficult for a user to know the true extent to which they have protected their profile by enhancing privacy settings, with many 'deluded' that they have adequately done so.⁷⁴ Moreover, suggesting that privacy has been waived by agreeing to a platform's *pro forma* privacy policy is clearly insufficient, given the 'information asymmetries' between the platform and user:⁷⁵ policies are agreed to but hardly read and inaccessible to the average reader, set to defaults favouring publication and unilaterally changed.⁷⁶

The above issues highlight the challenge of determining when a user truly has a 'reasonable

67 See also Computer Misuse Act 1990 as amended by Serious Crimes Act 2015.

68 RIPA s.26(2) and 26(9)(a) explain that surveillance is 'directed', thus usually entailing the need for a DSA, where it is 'covert but not intrusive'; 'covert surveillance' is defined as 'carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place.'

69 UK Home Office, 'Covert Surveillance and Property Interference: Revised Code of Practice August 2018' (2018) §§3.10-17.

70 RIPA s.26(2),(9)(a).

71 Edwards/Urquhart *supra* n. 38 p. 294.

72 *Ibid.*

73 Richard de George, 'Privacy, Public Space and Personal Information' in Ann Cudd, Mark Navin (eds.) *Core Concepts and Contemporary Issues in Privacy* (2018) p. 115.

74 Edwards/Urquhart *supra* n. 38 p. 295.

75 Kira Rønn and Sille Søre, 'Is social media intelligence private? Privacy in public and the nature of social media intelligence' *Intelligence and National Security* Vol.34 No.3 (2019) p. 366.

76 Edwards/Urquhart *supra* n. 38 p. 305.

expectation’ of privacy online, implying the need for surveillance authorisation. This has led to variance in policy amongst UK local authorities trying to comply with the legal framework when conducting OSINT activities for law-enforcement purposes. For example, some local authorities allow for up to 3 ‘looks’ at a unique user profile before a DSA is required;⁷⁷ others require a DSA for all subsequent visits after the first review,⁷⁸ or where monitoring takes place for longer than a week.⁷⁹ Lyle suggests that interpretive ambiguity has engendered a precautionary approach by law-enforcement officials, which may be welcome, but emanates from a lack of clarity in current legislation.⁸⁰

Reading-across to armed conflict settings

The analysis of the UK regulatory system above provides a case study of the complexity of situating OSINT operations within current legislative frameworks and IHRL obligations. While it is clear that OSINT operations have a wide capacity to engage and interfere with individual rights, domestic surveillance authorisation frameworks do not currently capture and regulate the full scope of what is possible. Accordingly, if such frameworks were applied to situations of armed conflict in order to fill the lacunae in IHL with regard to informational privacy, it is clear that a wide range of State-conducted OSINT activities would engage privacy rights, but with limited safeguards that are not technology-specific.

There are several further issues to overcome when attempting to incorporate these standards into the regulation of armed conflict. First, the extra-territorial application of IHRL obligations. Various authors have conceived of cyberspace as an ‘international space in which all customary international human rights apply’ – including the right to privacy – on the basis that States exercise jurisdiction there.⁸¹ When considering the applicability of privacy rights during active hostilities, it is logical – for ECHR States at least – to follow the position set out by the ECtHR in *Georgia v Russia (II)*: IHRL obligations continue to apply to acts which ‘produce effects’ extraterritorially, with the exception of ‘kinetic uses of force in the active phase of hostilities’.⁸² Accordingly, given that OSINT operations are largely ‘non-kinetic’ – impacting data confidentiality and privacy – it follows that IHRL obligations should continue to apply.

Second, the limitable and derogable nature of the rights to privacy and data protection. Watt notes that the war on terrorism has driven a ‘more permissive’ approach to limiting privacy rights in national security/surveillance contexts.⁸³ There are also limitations on data protection rules during armed conflict. For example, Geiß and Lahmann conclude that the EU’s General Data Protection Regulation (GDPR) can be partly or wholly disapplied by reference to a wide range of exceptions and restrictions on data subjects’

77 Wells/Gibson *supra* n. 17 p. 106.

78 Ryedale District Council, ‘RIPA and IPA Policy and Guidance Notes’ (2021) p. 27.

79 Lancaster City Council, ‘RIPA Policy and Procedure’ (2020) §5.9.

80 Alison Lyle, ‘Legal Considerations for Using Open Source Intelligence in the Context of Cybercrime and Cyberterrorism’, in Babak Akhgar, P. Saskia Bayerl, Fraser Sampson (eds.), *Open Source Intelligence Investigation* (2016) p. 281.

81 O’Connell *supra* n. 50 p. 23; Dapo Akande, Antonio Coco, Talita de Souza Dias, ‘Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies’ *International Law Studies* vol.99 Iss.4 (2022) p. 9.

82 O’Connell *supra* n. 50 p. 23; *Georgia v. Russia (II)* [GC], Merits, App.No.38263/08 [2021] §33.

83 Lubin *supra* n. 7 p. 488; Watt *supra* n. 55 p. 173.

rights.⁸⁴ However, where personal data is to be processed, regional courts have imposed strict necessity tests on States' ability to limit and derogate from data protection and privacy obligations.⁸⁵

Third, norm conflicts between IHL and IHRL's rules on privacy and data protection. There are a limited number of IHL treaty obligations that conflict with IHRL, for example, rules authorising special surveillance and censorship of POW correspondence.⁸⁶ While such norm conflicts require resolution on a case-by-case basis, for the most part, IHL is silent on issues of privacy and communications. This is partly due to the speed of technological advancement in this area, suggesting that the normative value of IHL's 'silence' entails that IHRL is used to gap-fill, subject to the limitations discussed above.⁸⁷

Conclusions

The above discussions highlight some of the legal and conceptual issues at play when assessing the lawfulness of OSINT operations in armed conflict. These include uncertainties in the *peacetime* IHRL framework that stem, in part, from persistent definitional uncertainties around open-source information and legal barriers precluding the application of IHRL in wartime. More recent UK policy appears to be responding to this by adopting a 'precautionary principle' in approaches to the use of such technology, including extraterritorially, in a manner comparable to law-enforcement operators: the British Army's stated policy is to apply RIPA to intelligence-gathering operations overseas on the basis that it 'provides a well-established regulatory framework...and reduces the chances of improper conduct and abuse.'⁸⁸ However, the consistency with which this principle is applied is unknown.⁸⁹ Accordingly, there remains a need for a more holistic framework protecting privacy and data in conflict contexts, which could, for example, be achieved through expanding the scope of current rules on cyber-hostilities and – as suggested above – re-examining the scope of the 'constant care' obligation in Art.57 API in order to bring IHRL standards into scope.

Part III - OSINT and Privacy: Non-state actors

This section considers the regulatory approach to the use of OSINT tools in armed conflict and humanitarian settings by non-State actors (NSAs), focusing on two case-study users: Bellingcat and the OSCE's Special Monitoring Mission in Ukraine (SMM). Whereas IHRL does restrain States in their capacity to infringe upon privacy and data protection rights to some extent, there are significant challenges with applying these legal standards to NSAs. In their absence, NSAs have begun to develop codes of ethics, but these remain piecemeal.⁹⁰ Bellingcat and the OSCE SMM provide an illustration of how these issues are conceptualised by two different types of NSA, although this is by no means an exhaustive survey.

Bellingcat

One prominent civil-society organisation (CSO) that is highly active in using OSINT techniques is Bellingcat, a self-professed 'intelligence agency for the people' based in the Netherlands whose work is

84 GDPR Rec.16, Arts.2(2),23. NB the Law Enforcement Directive (EU 2016/680) continues to apply safeguards to data processing and transfer by law enforcement.

85 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, CJEU Case C-73/07 [2008] §56; *Szabo and Vissy v Hungary* App.No.37138/14 [2016] §73.

86 GCIII Arts.76,92.

87 Lubin *supra* n. 7 p. 482.

88 Ministry of Defence, 'British Army Field Manual Volume 1 Part 10: Countering Insurgency' (2009) §12-20.

89 Wells/Gibson *supra* n. 17 p. 92.

90 Raymond *supra* n. 124 pp. 84,98.

geared both towards journalism and gathering evidence for future criminal prosecutions.⁹¹ The staff has described its approach as ‘passive monitoring’ of online material rather than intelligence-gathering.⁹² Some academics have criticised the potential for harm posed by Bellingcat’s investigations, citing as an example the ‘doxing’ of a criminal fugitive during public efforts to identify his whereabouts,⁹³ with ten Hulsen suggesting that such efforts risk circumventing legal safeguards on police investigations that preserve the criminal process and the rule of law from ‘vigilante justice’.⁹⁴ More recent developments in its practice indicate that Bellingcat is recognising these risks, avoiding deceptive tactics to penetrate digital communities or engage in digital ‘social engineering’ techniques, and using ‘sockpuppet’ (i.e., anonymous) social-media accounts when undertaking SOCMINT monitoring to preserve the identities of researchers, targets and third parties, particularly where identification could lead to real-world threats from hostile actors.⁹⁵ However, even using ‘sockpuppets’ could qualify as ‘covert’ OSINT according to the definition proposed by Edwards and Urquhart, and technically would violate Facebook’s terms of service – indicating that Bellingcat’s activities *do* continue to raise privacy-infringement risks.⁹⁶

Legal frameworks

During an armed conflict, Bellingcat’s civilian staff – assuming they are unconnected with and do not act for a party to the conflict – would continue to be bound by criminalised rules of IHL. They would also be bound by any domestic laws implementing IHL to the extent that they fall under the relevant State’s jurisdiction. Further, they may be indirectly obliged to comply with IHL rules by a host State that is required to ‘ensure respect’ for IHL in accordance with its obligation under Article 1 Common to the Geneva Conventions.⁹⁷ However, ambiguity over the IHL obligations of Bellingcat staff remains: for example, if they were to access confidential medical data of civilians via OSINT activities during an ongoing conflict but not in support of a conflict party, does it follow that they risk a breach of customary IHL?⁹⁸

Formally, Bellingcat’s human rights responsibilities are limited, given that IHRL is predicated on the principle of State responsibility. While there have been significant steps to bring NSAs – particularly corporations – within scope, such entities cannot yet be said to be formally bound by IHRL.⁹⁹ Nevertheless, the activities of Bellingcat’s staff may fall within the scope of the Netherlands’ positive obligation to guarantee the right to privacy of private individuals,¹⁰⁰ balanced against those staff members’ *own right* to freedom of speech.¹⁰¹ Furthermore, the CJEU has held that the EU Charter – which preserves the rights to privacy and data protection – can be invoked between private parties in

91 Higgins, *We are bellingcat: an intelligence agency for the people* (2021).

92 Interview with Bellingcat staff member, 4 August 2022

93 ‘Use of the internet to search for and publish identifying information about a particular individual, typically with malicious intent’ – Jeffrey Pittman, ‘Privacy in the Age of Doxing’ 10 *Southern Journal of Business & Ethics* (2018) pp. 53-4.

94 Ten Hulsen *supra* n. 48 p. 28.

95 Interview with Bellingcat staff member, 4 August 2022

96 Facebook, ‘Terms of Service’ §3.1.

97 Geneva Conventions, Common Art.1.

98 Marco Sassòli, *International Humanitarian Law: Rules, Controversies and Solutions to Problems Arising in Warfare*, (2019) p. 198-199.

99 Noam Schimmel, ‘The IHRL Responsibilities of NGOs’, *Oxford Human Rights Hub* (2015).

100 *Marckx v Belgium* 6833/74 ECHR 2 (1979) §31.

101 *Von Hannover supra* n. 61.

their horizontal relations, giving rise to ‘concrete legal obligations’ subject to, *inter alia*, a proportionality analysis.¹⁰² These developments in IHRL applicable at the State level suggest that privacy infringements could become more of a pressing consideration in the future for Bellingcat’s operations.

Approach

In the absence of a robust regulatory framework preserving privacy and data protection during OSINT activities, self-regulatory measures have developed. Bellingcat claims to adhere to the IMPRESS Standards Code for Journalists, which sketches a ‘reasonable expectation of privacy’ standard, as well as having an ethics board.¹⁰³ Accordingly, a more nuanced attitude to reasonable expectations of privacy online appears to be developing: staff has distinguished the privacy expectations attached to, for example, membership of a 30-person locked community group on Facebook versus a 30,000 open group, while projects are subject to a digital threat and risk assessment process as recommended by the Berkeley Protocol.¹⁰⁴ Bellingcat’s Ukraine TimeMap platform, available on its website, articulates this approach to privacy in an armed conflict setting.¹⁰⁵ It ‘plots out and highlights incidents that have resulted in potential civilian impact or harm’, drawn from social media since the Russian invasion in February 2022. As part of its methodology, the TimeMap imposes restrictions to safeguard privacy: obscuring the geolocations of sites by a few hundred metres, embedding source links so that they disappear when the underlying content is deleted by its original poster, and filtering out posts showing identifiable, immobile bodies – a principle that has its roots in IHL’s rules on respect for the dead.¹⁰⁶ This suggests that Bellingcat’s approach to privacy is evolving, but it does not consider itself directly bound by IHRL obligations. Instead, privacy-respecting practices are being undertaken primarily to ensure that digital evidence is not invalidated before international tribunals due to being obtained in an IHRL-infringing manner.¹⁰⁷

OSCE’s Special Monitoring Mission in Ukraine

The OSCE’s Special Monitoring Mission in Ukraine provides a useful comparison as an international organisation (IO) *acquiring, analysing, and disseminating* OSINT. Until its closure in 2022, the SMM was mandated under the Minsk Agreements to gather information and report facts in Ukraine’s partially-occupied Donbas region.¹⁰⁸ It deployed drones, along with OSINT and geospatial information analysts, to monitor adherence to ceasefire provisions, publishing extensive open-source reports and frequently releasing drone footage online for further analysis by CSOs and media,¹⁰⁹ although its mandate precluded attribution of responsibility to a conflict party.¹¹⁰ SMM staff have acknowledged the privacy and data protection ramifications of conducting drone flights over contested civilian areas. For example, publicly identifying local civilians crossing the Donbas Line of Contact at unofficial crossing points could result in punishment by the authorities and closure of crossings, with knock-on impacts on access to

102 Ten Hulsen *supra* n. 48 p. 17; *Association de Médiation Sociale*, CJEU Case C-176/12 [2014] §§41-3.

103 Bellingcat, ‘Kontakt’; IMPRESS, ‘Standards Code’ Art.7 Guidance.

104 Interview with Bellingcat staff member, 4 August 2022

105 Bellingcat, ‘Civilian Harm in Ukraine’ (2022).

106 Bellingcat, ‘The TimeMap Methodology’ (2022).

107 Rome Statute Art.69(7).

108 OSCE Permanent Council, ‘Decision No.1117 21 March 2014’ PC.DEC/1117 (2014).

109 Interview with former member OSCE Special Monitoring Mission to Ukraine, 30 July 2022

110 Walter Dorn, Cono Giardullo, ‘Analysis for Peace: The Evolving Data Tools of UN and OSCE Field Operations’, *Security and Human Rights* 31 (2020) pp. 95-6.

schools, workplaces, and services.¹¹¹ The SMM acknowledges that it lacked sufficient capacity to properly classify secure data collected on individuals,¹¹² while the use of private-sector subcontractors to operate long-range drones raises concerns about reliance on entities not adherent to humanitarian principles such as impartiality and respect for civilians.¹¹³

Legal frameworks

Compared with emerging jurisprudence applying customary international law to NSAs,¹¹⁴ the normative position is that IOs like the OSCE are not in general bound by IHRL obligations and are thus unlikely to be bound by privacy and data protection obligations, even though data protection rules are an ‘essential enabler’ of humanitarian IOs’ ‘do no harm’ mandate.¹¹⁵ Instead, a patchwork of data protection regimes has sprung up amongst major IOs, all of which fail to state whether they consider IHRL to constrain their data practices as a matter of law.¹¹⁶ The prevailing view is that privileges and immunities also shield IOs from meaningful domestic obligations concerning data protection.¹¹⁷ Here the picture remains fairly complex. For example, while IOs operating in the EU could claim immunity from the application of EU data protection rules such as GDPR, Kuner has flagged that Art.8 EU Charter describes data protection as a fundamental right, thus taking ‘precedence over international law, including international agreements’ and implying that GDPR could override IO privileges and immunities.¹¹⁸

Approach

In this context, the SMM’s activities suggest a somewhat limited – but developing – appreciation of privacy/data protection and ethics issues. A comprehensive approach to risk assessment was missing throughout their operations, with assessments only undertaken at a localised level to assess harm from potential drone crashes. While some efforts were made to obtain consent by discussing drone operations with community leaders,¹¹⁹ there appears to have been minimal appreciation for the potential harms associated with publishing even anonymised/aggregated data sets. This bears out the characterisation of SMM’s early drone operations in the Donbas as a ‘regulatory wild west’, as a former staff member has described it: a vacuum where legal restrictions were largely inapplicable and ethical constraints had not been fully established.¹²⁰ Future risk-mitigation approaches have been suggested if such projects are developed in the future, such as ‘locking in’ privacy-enhancing practices through data-minimisation

111 Interview with former member OSCE Special Monitoring Mission to Ukraine, 30 July 2022

112 Dorn/Giardullo, *supra* n. 110, pp. 96-97.

113 OSCE Code of Conduct 2003 Art.3; Rahel Dette (2018), ‘Do No Digital Harm: Mitigating Technology Risks in Humanitarian Contexts’ in Silvia Hostettler, Samira Najih Besson, Jean-Claude Bolay (eds.) *Technologies for Development* p. 22.

114 See, for example, the leading case before the Supreme Court of Canada regarding the applicability of international law obligations to corporate non-state actors, *Nevsun Resources v Araya* SCC 5 [2020] §107.

115 Christopher Kuner, ‘International Organisations and the EU General Data Protection Regulation’, *International Organisations Law Review* 16 (2019) p. 162.

116 Asaf Lubin, ‘Data Protection as an International Legal Obligation for International Organisations: The ICRC as a Case Study’ in Russell Buchan, Asaf Lubin (eds.), *The Rights to Privacy and Data Protection in Times of Armed Conflict* (2022) p.250; Kuner *supra* n. 115 p. 163.

117 Lubin *supra* n.116 p. 255.

118 Kuner *supra* n. 115 p. 184.

119 Interview with former member OSCE Special Monitoring Mission to Ukraine, 30 July 2022

120 *Ibid.*

policies, deleting unnecessary footage, and coarsening image resolution to >0.5m.¹²¹ More broadly, the SMM's drone-led OSINT activities highlight the urgent need for harmonised, enforceable legal and ethical standards across the range of IOs undertaking OSINT activities in armed conflict settings.

Conclusions

The two case studies explored here are illustrative, but by no means exhaustive, of the different regulatory contexts, operational realities, and ethical approaches of two non-State actors using OSINT in their operations. A more holistic analysis of a wide range of OSINT actors in this space would be an invaluable next step, but the above discussion is sufficient to highlight the key issue: the absence of applicable legal frameworks, including by force of IO privileges and immunities, delegates regulation of the use of OSINT to non-binding ethical doctrines and voluntary commitments, resulting in a fragmented approach between users based on a limited understanding of potential harms.

Part IV - Broader Issues

The above discussions indicate that real-world harms can emanate from uses of OSINT by States and non-States alike, where insufficient appreciation for their complex interaction with privacy and data protection rights persists. Additionally, it is worth flagging two emerging 'threat vectors' of the OSINT lifecycle that appear consistently in the literature: the 'Mosaic Effect' and the 'Consent Paradox'.¹²² Both emerge from the core concerns that this paper has identified regarding respect for and protection of individual privacy and data protection rights and are often unintended consequences of users' failings in those areas.

The Mosaic Effect

States and non-States alike demonstrate some level of understanding of the risks pertaining to Personally Identifiable Information (PII), given its centrality to contemporary data protection frameworks. However, risks are present even when data handlers act responsibly, for example, through the use of anonymisation and data-aggregation practices. For example, studies show that knowing as few as four data points is enough to re-identify 87-95% of people in a de-identified dataset, indicating that simple anonymisation may be insufficient to safeguard individual privacy.¹²³ Further, where different data types are combined together, inferences can be drawn that 'enable the...identification of...named and/or unnamed individuals [and] groups'. The amalgamated product, demographically identifiable information (DII), can be easily 'weaponised', as in the following example:

A humanitarian IO managing several IDP camps in Country C, affected by armed conflict, publishes a map showing camps with the largest influxes of IDPs across the country. The map intentionally obscures sensitive information about the location of a protection centre for demobilised child soldiers. However, a CSO known for assisting demobilised child soldiers at the centre publishes an online blog stating that it is providing its services at the camp in Country C, which has the largest influx of IDPs. Armed Group Y,

121 '0.5 meters is roughly the size of the human body as seen from above' – Eyal Weizman, *Forensic Architecture: Violence at the Threshold of Detectability* (2017) p. 28.

122 Joseph Guay, Lisa Rudnick, 'Open Source Investigations: Understanding Digital Threats, Risks, and Harms' in Sam Dubberley, Alexa Koenig, Daragh Murray (eds.) *Digital Witness* (2019) p. 304.

123 Raymond *supra* n. 124 p. 91; UN OCHA, 'Humanitarianism in the Age of Cyber-Warfare', *OCHA Policy and Studies Series II* (2014) p. 15.

*seeking to recapture child soldiers, ‘cross-corroborates the de-identified map with the...de-identified blog’ to locate the children digitally before attacking the camp and kidnapping them.*¹²⁴

This is an example of the ‘Mosaic Effect’ in action, whereby an individual, de-identified dataset in isolation may not pose a threat of identifying an individual, but combined (‘mosaicked’) with other datasets can reveal sensitive information about people or groups.¹²⁵ Managing this risk, in order to avoid adverse effects of OSINT by IOs in armed conflict settings, calls for significant expansion of the use of data protection impact assessments and better inter-organizational coordination on DII in humanitarian settings.

The Consent Paradox

Informed consent relating to the use of information presents a second ‘threat vector’ for the acquisition, processing, and sharing of OSINT.¹²⁶ This is a particular problem for humanitarian organisations, given the principle of humanity that guides their work.¹²⁷ For States, by contrast, exemptions or limitations may justify avoiding consent obligations. Nevertheless, there will be situations where obtaining informed consent is a political and ethical imperative – e.g., where a State is an occupying power in another territory and is trying to ‘win the hearts and minds’ of communities while preserving security or contributing to a UN peacekeeping mission.

Problematically, techniques such as OSINT are more likely to be used where other approaches to data-gathering are impossible, such as in conflict zones. This gives rise to a ‘consent paradox’ – actors are forced to ‘impossibly balance’ the expectation of obtaining informed consent with the ‘operational requirements of working in inherently non-permissive environments.’¹²⁸ This is added to existing challenges regarding whether information acquired through OSINT is publicly-available, while expectations may also vary between communities, making ‘informed’ consent quite a subjective criterion.¹²⁹ Given these challenges, Greenwood et al. have suggested a reasonable consent standard may have to suffice: ‘persons have the right to be *reasonably* informed about information activities during all phases of information acquisition and use.’¹³⁰ However, the above discussion makes it clear that a coherent understanding of how these threats emanate from the use of OSINT by States and NSAs alike in armed conflict and conflict-affected settings is still lacking. Ultimately, as Sandvik and Raymond have noted, developing a more coherent ‘theory of harm’ focused on ‘potential deleterious impacts resulting from current technical realities’ is an essential preliminary step.¹³¹

124 Raymond *supra* n. 11, p. 93-95.

125 OCHA *supra* n. 123 p. 15; Jill Capotosto ‘The Mosaic Effect: the revelation risks of combining humanitarian and social protection data’, *ICRC Humanitarian Law and Policy* (2021).

126 ‘Voluntarily and freely given based upon a clear appreciation and understanding of the facts, risks, implications and future consequences of an action’ – ICRC, ‘Professional Standards for Protection Work’ (3rd ed. 2018) p. 127.

127 ICRC *supra* n. 42 p. 3.

128 Raymond *supra* n. 124 p. 97.

129 UN Global Pulse ‘Meeting Report: “Improving Data Privacy & Security in ICT4D” A Workshop on Principle 8 of the Digital Development Principles’ (2015) pp. 7-8.

130 Faine Greenwood, Caitlin Howarth, Danielle Escudero Poole, Nathaniel Raymond, Daniel Scarnecchia, ‘The Signal Code’, *Harvard Humanitarian Initiative* (2017) p. 17.

131 Sandvik/Raymond *supra* n. 15, p. 16.

Conclusions

This paper has considered the use of OSINT in armed conflict settings by three key user groups with differentiated legal responsibilities, priorities, and aims. It has focused on threats and harms from OSINT, but it is worth reiterating that OSINT also presents an enormous opportunity to embed better implementation of IHL, protect civilians and fulfil human rights by rebalancing information asymmetries that advantage State actors. The starting point has been to highlight continuing uncertainties in how OSINT/OSIF and related terms are defined. This stems from issues with the understanding of when digital information is ‘publicly available’, and with conceptualising methods of data acquisition as covert or overt. This uncertainty clouds a better understanding of the harms and emerging norms associated with the use of OSINT.


For States, we have seen how existing privacy/data protection responsibilities under IHRL and domestic legal frameworks regulating surveillance activities provide *some* protection against the harms that the unregulated use of OSINT can entail. However, persistent conceptual difficulties around the definition of OSINT and the situation of these activities within the remit of domestic surveillance authorisation frameworks remain major problems. The resulting situation is one where contemporary privacy law is unable to fully capture OSINT activities within its scope. This is particularly obvious in armed conflict settings, where IHL provides limited restraint, necessitating *renvoi* to IHRL and its articulation in domestic law and jurisprudence.

Clearly, a more holistic State-by-State analysis will be a necessary next step – something that this paper calls for. While the *status quo* appears to favour approaching privacy in wartime on the basis of a precautionary principle, this is unsatisfactory and no replacement for a transparent, future-facing, and accessible legal authorisation framework. One viable approach suggested has been to use the ‘constant care’ obligation in Art.57 API as an entry point for bringing privacy rights within the scope of IHL in order to regulate OSINT more directly.¹³² For non-States, particularly those working in armed conflict settings with a humanitarian agenda, legal restraints are much more limited and uncertain. The patchwork of guidance on privacy/data protection highlights a deeply fragmented approach with major threat vectors for unintended harms that need regulating in a harmonised manner.

One of the core issues common to both States and non-States is the fundamental, definitional challenge to traditional notions of privacy and data protection that open-source information poses. Practical solutions exist here: clarifying the scope of application of data protection rights under IHRL, tailoring domestic surveillance authorisation frameworks to handle publicly-available information better, and consolidating legal and ethical guidance across all CSOs/IOs operating in humanitarian settings. Ultimately, a necessary precursor to these is the development of an evidence-based ‘theory of harm’, adapted to the possible negative impacts arising from the applications of ICTs generally – and OSINT specifically – in armed conflict contexts.¹³³ Equipped with a more nuanced understanding of the risk-opportunity profile OSINT presents, and with the development of the legal and ethical frameworks, OSINT can continue to be a paradigm-shifting tool, tackling information asymmetries while also protecting individuals and communities from harm.

¹³² Asaf Lubin ‘The Duty of Constant Care and Data Protection in War’ in Laura Dickinson, Edward Berg (eds.), *Big Data and Armed Conflict: Legal Issues Above and Below the Armed Conflict Threshold* (2022) p. 8

¹³³ Sandvik/Raymond *supra* n. 15, p.16.



This article was published by the Security and Human Rights Monitor (SHRM).
www.shrmonitor.org.

Security and Human Rights (formerly Helsinki Monitor) is a journal devoted to issues inspired by the work and principles of the Organization for Security and Cooperation in Europe (OSCE). It looks at the challenge of building security through cooperation across the northern hemisphere, from Vancouver to Vladivostok, as well as how this experience can be applied to other parts of the world. It aims to stimulate thinking on the question of protecting and promoting human rights in a world faced with serious threats to security.

Netherlands Helsinki Committee
Het Nutshuis
Riviermarkt 4
2513 AM The Hague
The Netherlands

© Netherlands Helsinki Committee. All rights reserved.

www.nhc.nl