Scientia Militaria, South African Journal of Military Studies, Vol 50, Nr 1, 2022. doi: 10.5787/50-1-1345

Social media intelligence: The national security–privacy nexus

Dr Dries Putter
Department of Strategic Studies, Stellenbosch University &
Affiliate Member, National Security Hub, University of Canberra

Dr Susan Henrico
Department of Strategic Studies & Research Fellow SIGLA,
Stellenbosch University

Abstract

Globally, changes in technology have always shaped the intelligence collection environment. South Africa is no exception. The emergence of satellite imagery had a significant influence on geographic intelligence (GEOINT) capabilities and, similarly, the emergence of the telegram and later the telephone had an equally significant effect on the signals intelligence (SIGINT) environment. With communications being revolutionised by mobile technology, such as recording, geo-positioning and photography, collection and distribution are ubiquitous. Smart mobile communication technology is also the driver of social media everywhere – at all ages, for state and non-state purposes, non-stop. More recently, social media intelligence (SOCMINT) became a key content domain for exploitation by the intelligence community. Examples of the successful exploitation of SOCMINT can be found internationally. It would be surprising if South Africa is not yet a statistic in terms of this phenomenon. Initially, many organisations viewed (and some still do) SOCMINT as an open-source intelligence (OSINT) tool. However, when considering the South African (SA) intelligence landscape, the concepts 'democracy', 'transparency' and 'intelligence oversight' are calibrating factors to bear in mind. It is also important to consider the influence of the national legislative framework governing the use of SOCMINT in South Africa. It then becomes clear that issues – such as the right to privacy – mean that SOCMINT is probably no longer covered by the scope of the OSINT definition and that intelligence organisations collecting social media content and producing SOCMINT should adhere to the legislative framework governing the collection and use of social media content and the production of SOCMINT. This article argues that SOCMINT and OSINT should be separate collection domains to protect the imperative of the right to privacy and national security requirements in a balanced manner by means of unambiguous national regulation in the interest of all citizens.

Keywords: social media, social media intelligence (SOCMINT), open-source intelligence (OSINT), national security, intelligence, privacy, POPIA, RICA, South Africa

Introduction

Social media can no longer be regarded as a niche technology or social interaction enabler. It is mature to the point of being weaponised – with the current usage thereof in the Russia–Ukraine war a case in point[67] – the naïve intent of the developers of some or all the current social media applications aside. Social media in the contemporary age is a significant enabler of social cohesion, cultural diversification, trade, security and access to and interaction with almost everything. Significant portions of the daily lives of people, young and old, are dedicated to interaction with one or a variety of social media applications. This might not seem to be very problematic from a developmental perspective. However, when the other side of the nexus is introduced – security and its older brother, national security – then the conversation becomes complex. Social media applications and the content thereof are currently utilised to its capacity by international alliances, individual countries and individuals in support of their preferred protagonist in the Russia–Ukraine war:

> Social media has become a primary source of information for news-hungry audiences around the world trying to make sense of the Russian invasion of Ukraine. At the same time, it's being used by the governments of Russia and Ukraine to set the agenda for wider media reporting. Official Russian government accounts have been found to be amplifying pro-Russia disinformation on Twitter. Meanwhile, the Ukrainian government has taken to the platform to appeal to its two million followers for support.[68]

Defining social media also still seems to be problematic. Social media is inclusive of another construct – social networking.[69] Social networking can be defined as "a community that forms around a common interest",[70] whereas social media is inclusive of "social networks, blogs, wikis, podcasts, fora, content communities and micro-blogging".[71] Considering these descriptions, the problem around the need for privacy (or exclusion of those not part of the 'common interest') and the need for transparency about such 'common interest' from a security perspective, are easily imagined. The above-mentioned problem or social dilemma can only be regulated with contractual agreements and legislation.

Today, and progressively towards the horizon of time, social media both enables social interaction and facilitates insecurity on an international scale. Social media is instrumental in building social cohesion around common interests, but it also facilitates the destruction of social cohesion when manipulated by state and non-state actors with dubious intent. This fact can best be illustrated by referring to the current Russia–Ukraine war, which has polarised the international community yet again into West vs East or democratic vs authoritarian or communist. Social media will never be regarded as just another platform for conversation, but rather as the 'go-to' platform to shape narratives within every state power domain to secure national interest. It is thus a primary national intelligence enabler.

The article introduces, for the benefit of the uninitiated to this phenomenon, social media intelligence (SOCMINT)[72] and presents arguments about the possible impact social media data, information and knowledge (henceforth referred to as 'content') have on the intelligence community, privacy concerns and national security. Assisting the reader to differentiate between SOCMINT and open-source intelligence (OSINT) – a key objective of this article – the discussion is expanded into relevant semantics within the SOCMINT–OSINT debate. This also serves to highlight the requirement for robust legislation to regulate the use of SOCMINT as a process and product. The article introduces a fundamental differentiating element between SOCMINT and OSINT – citizens' right to privacy in a nexus with national security imperatives of states. The second objective of the article is to consider leading international SOCMINT regulations as a benchmark of how this national security–privacy nexus within the SOCMINT–OSINT debate informs an introductory discussion about the SA legislative framework, which is central to the regulation of the use of SOCMINT within the SA context. The article does not constitute a legal opinion, but rather an opinion about what South Africa must consider for an enhanced balance of the national security right to privacy nexus within the context of the SOCMINT–OSINT debate.

The birth of SOCMINT

Accepting the existence and maturity of the internet[73] and the World Wide Web application, a significant by-product of this globally distributed communication and content storage capacity is social media. Britannica (2021) provides a very apt description of the internet, namely "a system architecture that has revolutionized communications and methods of commerce by allowing various computer networks around the world to interconnect"[74]. An important fact not to miss is that Britannica (2021) estimated that, by 2020, more than 4,5 billion people had access to the internet – and consequently to all associated applications. This figure will grow exponentially. It is the urge of individuals to communicate that drives the proliferation of social media applications and their use. The internet and now ubiquitously used World Wide Web applications are most probably the most powerful communication tool known to humankind. This holds incalculable potential for intelligence operations but similarly, and in parallel, an almost uncontrollable communication medium for (national) security threats. A recent example is the tremendous influence that social media had and still is having on health intelligence. While governments are trying to influence their citizens positively to vaccinate, so-called 'anti-vaxxers' are spreading a different picture via social media. It is clear that social media can have both a positive[75] and a negative effect on the spread of information about health issues.

The acronym 'SOCMINT' was coined by Omand, Bartlett and Miller in 2012[76] who argue:[77]

> In an age of ubiquitous social media it is the responsibility of the security community to admit SOCMINT into the national intelligence framework, but only when two important tests are passed. First, that it rests on solid methodological bedrock of collection, evidence, verification, understanding

and application. Second, that the moral hazard it entails can be legitimately managed.

Ten years on, SOCMINT is significantly influencing political, socio-economic and national security dynamics to the point of facilitating instability. Such instability was experienced during the Arab Spring campaigns (2010-2011[78]), not necessarily due to access to social media, but rather facilitated and developed using social media.[79] Senekal (2018) provides a short summary of such influence –

> Twitter, for example, is used by the Islamic State of Iraq and Syria (also known as the Islamic State of Iraq and Al-Sham, currently known as Daesh) (ISIS) and by Al-Qaeda's affiliate, Al-Shabaab. By 1999, almost every known terrorist group had a presence on the internet and during the 2011 Egyptian Revolution 32 000 new groups and 14 000 new pages were created on Facebook from within Egypt. Significant mass demonstrations where Twitter played an important role include the civil unrest in Moldova in 2009, the Iranian election protests of 2009–2010, the Tunisian Revolution of 2010–2011, the Egyptian Revolution in 2011 and the Occupy Wall Street (OWS) protest, which took place in the autumn of 2011 in cities around the world. Locally, a lot of conversations around recent movements such as #RhodesMustFall and #FeesMustFall also took place on social media and especially on Twitter.80

Brown, Guskin and Mitchell (2012) state, "[s]ocial media indeed played a part in the Arab uprisings. Networks formed online were crucial in organising a core group of activists, specifically in Egypt. Civil society leaders in Arab countries emphasised the role of "the internet, mobile phones, and social media"[81] in the protests. Additionally, digital media have been used by Arabs to exercise freedom of speech and as a space for civic engagement."[82] These examples could be expanded into a significant volume of pages when the current war in Ukraine is brought into view from the perspective of SOCMINT and the use of OSINT. Several other researchers have investigated this phenomenon. The instability and change facilitated by social media are not the focus points of this article, but rather the implications of SOCMINT, operationally and legally. Several years after the article by Brown et al., (2012)[83] and Smidi and Shahin (2017) concluded:

> [T]he bulk of the research contends that social media enabled or facilitated the protests by providing voice to people in societies with mostly government-controlled legacy media; helping people connect, mobilise and organise demonstrations; and broadcasting protests to the world at large and gaining global support. Some scholars, however, argue that social media played only a limited or secondary role, which ought to be viewed alongside other social, political, economic and historical factors.84

Social media therefore has an incontestable influence on national security issues. This could be viewed solely from a negative perspective, but a more prudent approach would

be to consider both opportunities and threats associated with social media within the context of national security and intelligence. Consideration of these factors should inform conversations about mitigation of threats and exploitation of opportunities within a national legal framework. In South Africa, such legal framework is still in the infant stage of development. This results in possible uncertainty about the impact on the use of SOCMINT by SA intelligence agencies. First, let us delve into potential SOCMINT semantics and opportunities on offer by this ubiquitous technology and software.

Critical semantics

A question could be raised whether SOCMINT is open-source intelligence (OSINT). Hassan argues, "OSINT sources are distinguished from other forms of intelligence because they must be legally accessible by the public without breaching any copyright, patents or privacy laws."85 Social media stores and provides access to considerable amounts of content; yet vast volumes of such are privileged, i.e., protected by personal passwords and administrative rights as well as copyright protection agreed to in application terms of reference.

> Frequently, 'unrestricted' data on these public social media sites is restricted by individual privacy settings; for instance, Facebook notifications by an individual are accessible to only those within the individual's peer group if the privacy setting is established in such a manner. However, SOCMINT, by definition, accesses all such data without considering privacy. This places a greater emphasis on SOCMINT's instructions for dealing with individual privacy than that of conventional OSINT searches. Even though OSINT does intrude on individual privacy when it stores search information made by individuals, such as the information that is sought when searching for a location on an Internet map. However, SOCMINT's intrusion is far more incisive than [that of] OSINT, because it monitors people in the most obtrusive manner and in their most unaware state – when they are interacting and relaxing in their online social comfort zone.[86]

SOCMINT is therefore not a new phenomenon. However, SOCMINT is still regularly assumed part of OSINT. Considering the perspectives already aired, SOCMINT can probably not be regarded as OSINT, and hence the conversation about the legal basis for SA intelligence services and agencies to gain legitimate access to the content of social media in support of national security imperatives.

In an article in the *Daily Maverick*, it is stated how the SA government is using content from social media accounts, claiming that it is used against security threats. The data are bought from surveillance companies, who in turn bought it from social media companies.[87] If a significant part of such data were privileged (i.e., access authority required), the question could be raised whether SOCMINT can be viewed as OSINT (no access authority required) or rather as a new collection discipline with its own set of rules that consider the ethical and legal requirements of privacy. From a definitional perspective – OSINT is outlined and characterised as "information that is publicly

available to anyone".[88] Constantin-Sorin (2019) argues that this includes "traditional media (newspapers, radio, television, etc.), public data (government reports, official data, etc.), web communities and personal reports".[89] Key to this definition is the construct of publicly available, which is different from having account access.

One perspective defines SOCMINT as "information gathered from social media sites and the tools employed to analyse this data [and] focuses on understanding and forecasting behaviours, crises, and events".[90] This definition provides little insight into the level of intrusiveness and does not differentiate SOCMINT from, for example, OSINT. A more widely articulated perspective is that SOCMINT can be defined and characterised as –

> [T]he process of identifying, collecting, validating and analysing data from social media sites and accounts using nonintrusive and/or intrusive methods to develop intelligence that reduces the unknowns in the decision process[91] [and/or] with the aim of developing products for national security.[92]

Key to this definition is 'accounts', which implies access authority required or privacy or privileged content. The differentiation is therefore focused on the process rather than on the products generated.

The confusion about whether SOCMINT can be regarded as an OSINT discipline possibly originates from the fact that some might regard content that is openly shared on social media platforms as 'publicly available to anyone'. When considering the OSINT definition by Lowenthal and Clark,[93] some of the elements of SOCMINT are contained in the OSINT definition. However, when considering the explanations provided by Davis (2015)[94], Ivan, Iov, Anamaria, Codruta and Nicolae (2015)[95] and Constantin-Sorin (2019)[96] it is no longer clear whether SOCMINT can be grouped within the OSINT discipline. In short –

> SOCMINT [in other words the process of collection and exploitation] can be deployed on content that is private or public, while OSINT is about strictly publicly available content, such as articles, news sites, or blog posts, published in print and on the open internet and clearly intended and available for everyone to read and watch. SOCMINT requires more specific regulation, policies and safeguards that take into account the very unique and specific nature of social media: a privately-owned space (i.e., owned by private companies) where people share freely.[97]

Consideration should be given to both international and legal aspects governing the use of social media as an intelligence source before drawing any such conclusions. This distinction and classification should inform future policy decisions about the mandates of intelligence services and agencies, as well as subsequent organisational restructuring (if required) and resource allocations. No matter how academics and experts eventually agree on a universal definition of SOCMINT, the phenomenon provides several opportunities. There are, however, also some moral and ethical issues.

SOCMINT and privacy

Without wandering into the never-ending maze that is constructed from morality and privacy, arguments are forwarded by Rønn and Søe (2019) with regard to the duality of social media.[98] These authors contend that social media has both a public and private character and where these two domains overlap, it creates a 'grey zone'. It is exactly this grey zone constructed of private content within a public space that separates OSINT from SOCMINT. Entry into this grey zone will require the verification of credentials, which separate it from the domain of OSINT. Rønn and Søe (2019) argue further:

> Although the information can easily be accessed, the pressing question is whether and under which circumstances it is morally permissible for government authorities to gain access to personal social media accounts and exploit the information for safety and security issues.[99]

Rønn and Søe (2019) refer to the opinions of Herman Tavani[100] about the types of privacies ("informational privacy is just one of four distinct kinds of privacy, the others being physical/accessibility privacy, decisional privacy and psychological/mental privacy"[101]) pointing out that information privacy is not a monolith within questions of morality.

> Informational privacy is often described as the ability to control or restrict access to one's personal information. Hence, in informational privacy it is personal information (or personal data) which people have a right to or an interest in having protected[102]

People also have an interest to protect the other 'rights to privacy'; yet society accepts that these will be violated by the state (within the parameters of national legislation) if such privacies pose a danger to the individual and/or to national security. The public spaces are also monitored with camera technology whilst monitoring the movement of both vehicle and people traffic through the streets in order to have a very quick response to incidents of terrorism perpetrated by (for example) knife-wielding psychopaths in the United Kingdom.[103] These psychopaths will have all their rights violated by the state once in custody – without public outcry, forgetting that individual privacy in public spaces was violated with surveillance by the state in order to provide some level of security. This cannot possibly be different for state surveillance of social media (cyber spaces) in order to have a reasonable response time for the purpose of security within the context of national interest. Yet, people seem to be less accommodating when it comes to their Facebook profile, Google browsing history or Twitter feed, forgetting that they hand over hard-earned private funds to the state revenue collectors to fund the state national security mandate. This nexus between public safety and individual privacy concerning the collection and exploitation of SOCMINT could be balanced with robust public consultation and unambiguous legislation because it is also in the public interest (as taxpayers) to get the security benefits locked up in SOCMINT opportunities. Such a balance should specifically consider the implications of state surveillance that is conducted "with or without evidence or reasonable suspicion – that is, whether the

surveillance is targeted or not".[104] Rønn and Søe (2019) write, "it might be morally permissible to access social media profiles in cases where the officials have a reasonable suspicion of criminal behaviour, it is much more morally problematic if the surveillance is conducted on random citizens".[105] Public dismay about intrusions on privacy by the state is thus less about what may be revealed than about being perceived as a criminal or national security threat. The fact that informed consent locks the state out of the available social media content does not minimise such perceptions of criminality of national security threat; it probably increases it. This dilemma could potentially be mitigated by robust legislation.

Privacy in cyberspace is therefore about securing legitimate access to personal content.[106] It could also mean legitimate access to private content by the state if legislation allows and regulates such access with unambiguous parameters of such legitimacy. The restriction of access to private content in cyberspace (typically in the social media space) is therefore a question of assigning or legislating for 'informed consent'[107] for the use of personal information. Such consent could be assumed implicit in legislation that allows the state to access personal content for the purpose of national security because in democratic societies, such as South Africa, the government is elected by the people to develop and protect the interests of the people.

> [W]e have to consent to others gaining access to our personal information. Informed consent is a central concept when addressing the question of informational privacy on social media platforms. Users give the specific platform their consent to allow the companies to access and use their personal information which is available on the specific platform. However, if it is possible for the platforms to infer new personal information, as argued above, it becomes difficult if not impossible to restrict access to and control over the flow of such information.[108]

SOCMINT opportunities

To support the proposition that social media is a social common with SOCMINT opportunities not yet experienced since the advent of intelligence as a construct, DataReportal (2022) rated Google first, YouTube second, and Facebook third as the world's most visited webpages, with Instagram and Twitter amongst the top ten[109] in October 2021. Facebook alone "had 2.910 billion monthly active users in October 2021" awarding it first place among social media applications, internationally.[110] The importance of Facebook, as a SOCMINT content goldmine, is in the broad approach the application has to social interaction. Facebook provides a platform that allows users to disclose any personal data and preference in virtually any media format. This results in in-depth conversations, photo sharing and video conversations, geo-positioning disclosure (checking in) and access to (unless blocked) friend networks. Before D-Day landings during World War II, the allied intelligence services used postcards and photographs taken during holidays to construct an accurate picture of the (then) current state of the area targeted for the landings.[111]

> The request [for such postcards and photos] came in 1942, with Brits desperate to help the war effort sending in 30,000 packs of pictures of the French coast within just 36 hours. Incredibly, by 1944, 10 million holiday snaps and postcards, hotel brochures, letters and guidebooks had arrived by post. [112]

It took the allied intelligence services approximately two years to amass 10 million items that graphically illustrated some part of the targeted landing area. In contrast, and significantly so, during 2013 (almost a decade ago now), Facebook achieved 350 million photographs daily.[113] To take it to a meta-level, *circa* 2020, it was said that the "chances are you see (and forward) some of the more than 3.2 billion images and 720,000 hours of video shared daily".[114] It is difficult to describe in words the opportunity locked up in that volume of content. This figure does not include the SOCMINT in text conversations and personal data continuously available and updated. The force multiplier or exponential enabler that should be noted with this vast mega volume of SOCMINT is that it is available on any smart device, anywhere and anytime, and now coming to the user via cloud services.

Contextually, with access to this amount of content – continuously updated – intelligence organisations worldwide can construct detailed target profiles without placing these organisations in harm's way during content collection or sacrificing plausible deniability – as would be the case when using human intelligence (HUMINT). A meta-perspective underscores the opportunities that SOCMINT facilitates:

> [To] contribute decisively to public safety: identifying criminal activity; giving early warning of disorder and threats to the public; or building situational awareness in rapidly changing situations. As society develops and adopts new ways to communicate and organise, it is vital that public bodies, including law enforcement and the intelligence community, keep up with these changes.[115]

This scenario is currently operationally active in the Russia–Ukraine war. Heidi Swart (2021) writes, "[y]ou can download your personal information – over 50 data categories – stored since you first joined. Posts, messages, tags, pokes, searches, the friended, the unfriended, login locations, facial recognition data."[116] The portfolio of information categories collected and available on each individual Facebook user can be found on the Facebook application under the Help section[117] (a link is provided in the endnotes). If you have access to this, then those more capable within the cyber domain certainly also have access to this information. Facebook (amongst several other very popular applications) therefore provides intelligence services and agencies with vast volumes of content on all possible indicators with which threat profiles can be constructed. The SOCMINT opportunity load is so extensive that the National Guard in Russia (Rosgvardia) is training Russian Army specialists as SOCMINT operations[118] specialists. The Rosgvardia commander-in-chief rather candidly notes, "[t]he creation of the National Guard is an answer to the threat posed by techniques of so-called non-violent resistance."[119] From a very pragmatic perspective, SOCMINT therefore provides

a credible source of content that could be used for the execution of national security threat detection, according to the Russians. Russia is a member of BRICS; so is South Africa. The BRICS partnership is consequently a perfect vehicle of international co-operation to exchange expertise on the matter of SOCMINT. However, in view of the recent Russia–Ukraine war and the considerable support Ukraine is getting from the international community, it would be ill advised for South Africa to support Russia with any kind of intelligence if South Africa is going to maintain a neutral position in this conflict.[120]

A similar, but different application within the intelligence environment, China's Social Credit System seek to regulate an individual behaviour-based score on the back of various social interaction activities.[121] Without getting into ethics and morality and questions about good and bad behaviour, a more relevant question within the context of this article would be what this has to do with SOCMINT. The answer and opportunity for intelligence organisations are that individuals are vetted continuously on as many aspects as possible within the parameters of the software and those regulating it. Over time, this should offer a platform that provides transparency about those that are trustworthy and those that are still working to get to that level. Very contentious? Not really, as national financial credit organisations do similar vetting, albeit more focused on financial management behaviour. The more incentive there is for the citizenry to live as 'good citizens' in the social media space, the more trustworthy the social media content therefore becomes to the point where it supports SOCMINT as an A-level source.

Social media is also used effectively in humanitarian operations. Crowdsourcing is an example where the public could provide real-time information on what is happening on the ground in a crisis.[122] Crowdsourcing has already been used effectively to outline areas where maps of such areas were, for instance, outdated.[123]

Another opportunity is locked up in the ability to manipulate content online and almost real-time as part of deception (a primary function within the counter-intelligence stable). The downside is that every opportunity available to state intelligence organisations is also available to every other state and non-state actor with adversarial intent. Several of these are classified as national security threats.

When considering the social media characteristics as discussed by Stegen, the usefulness of social media as a non-kinetic weapon is not a bridge too far. When affordable, user-friendly, interactive content is available with no state censorship in play (implying that distributed content "is not verified and false information can spread in this manner"[124]) – adversarial or malicious activities can be directed at targets of any size. This can be achieved by a variety of threat actors ranging from bored and/or inquisitive children to sophisticated terrorist and/or extremist organisations.

SOCMINT national security threats

The constant flux of societal dynamics of which Bauman (2006)[125] speaks, and which is quoted by Stegen (2019)[126], drives opportunity and threat. Changes within society are natural phenomena and have many drivers, such as the creation of knowledge and

technology. Change itself is not necessarily the threat, because change can be very healthy – a case in point is the 1994 leap into democracy in South Africa. That change was not driven by social media because social media did not exist yet. In contrast, the changes associated with the Arab Spring revolutions (2010-2011) might have had normal political and socio-economic triggers, but abnormal change propagation enabled by social media.[127] Although the triggers might have been typical during the Arab Spring, the effective mining of social media content could have revealed the tempo of the need for change, the planned tactics, the leadership involved, amongst several other aspects. Intelligence analysists would use the typical - *who, what, where, when, how, what thereafter and with what effect- type* of questions to support their analysis. Social media content collected from, for example, Facebook could have provided significant content to each of these questions. Other national security threats that could typically use the capabilities provided by social media are the spreading of fear through terrorism and extremism, subversion, deception and misinformation from the covert action playbook through the spreading of deep-fake content that could influence the outcome of an election or the credibility of national leadership. For example, espionage, through the posting of simple and/or coded content, enables the discovery of new technology, movement of armed forces, infrastructure vulnerabilities, resource shortages, human rights abuses, to name but a few.

International regulation of SOCMINT

International intelligence organisations seem to be perplexed and, in some cases, hamstrung by the legislative protection of privacy within the context of social media. This is of obvious concern to these organisations since their mandate to provide the state (and by implication the citizenry) with early warning about impending (national) security threats and various social media applications could be used as a legitimately privileged (and encrypted) communication medium between state or non-state threat actors.

An example noted by Hassan (2020)128 of transnational data protection legislation is the General Data Protection Regulation (GDPR) of 2018 promulgated by the European Union.129 Ben Wolford130 is of the opinion that the GDPR, comparatively speaking, constitutes a significantly robust data security regulation. The GPPR was promulgated to guarantee personal data security EU-wide, with noteworthy financial sanction power as deterrent to any prospective data collector. The GDPR is a logical extension of the European Convention of Human Rights (1950) that pursues personal privacy.131 In the 1950s, up until the advent of the internet, such a guarantee might have seemed plausible. This prospect changed significantly with the development of the now mature World Wide Web and its associated social media platforms. Hence, there is stronger regulation by the EU, i.e., the GDPR. Ironically, it was a privacy dispute with Facebook that triggered the development and promulgation of the GDPR.[132] In fact, according to Wolford (2021)[133], the GDPR applies to any entity that processes any personal data of any EU citizen, a truly transnational privacy regulation. This obviously has far-reaching implications for the operationalisation of the SOCMINT construct, since the successful execution of SOCMINT is premised on access to social media content. The GDPR

could also be perceived as a deterrent against the United States breaching the privacy of European citizens premised on the fact that most of the social media platforms originate from the United States.

At risk of entering a discussion about the entire GDPR regulation, it is worth mentioning the data protection principles contained in the regulation (Article 5(1–2)), namely:

> Lawfulness, fairness and transparency – Processing must be lawful, fair, and transparent to the data subject. Purpose limitation – You must process data for the legitimate purposes specified explicitly to the data subject when you collected it. Data minimization – You should collect and process only as much data as absolutely necessary for the purposes specified. Accuracy – You must keep personal data accurate and up to date. Storage limitation – You may only store personally identifying data for as long as necessary for the specified purpose. Integrity and confidentiality – Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption). Accountability – The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.[134]

The very first principle is already problematic for the intelligence organisation that seeks to maintain secrecy of its intent and targets. For the same reason as the first, the second principle is also contentious within the domain of intelligence collection and the complexity of national security. The third principle is aligned with the responsibility of intelligence collectors. The fourth principle, however, is out of kilter with how intelligence processors manage their content. They would typically hold onto that content for as long as possible and hopefully be able to keep on updating the content to keep it relevant. Security, integrity and confidentiality of the collected data are not hampering factors. However, because several of the principles are not aligned with how intelligence organisation's function, the last principle cannot be guaranteed. This briefly illustrates the privacy–national security nexus.

Social media legislation could be perceived as widening the chasm between the two competing social imperatives, i.e., privacy as a human right and security as a human right. The right to privacy according to the GDPR are –

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.[135]

Again, it is clear how these rights obliterate the potency of SOCMINT within the context of national security.

When considering the treatment of SOCMINT as an intelligence content domain, the United States experiences similar popular resistance against the surveillance of US citizens' social media. Law enforcement agencies use private service providers, such as Media Sonar, to survey social media and then just buy the data for SOCMINT purposes.[136] This resulted in social media companies, such as Facebook, Twitter and Instagram, adding specifications to their terms and conditions that explicitly prohibit the release and use of their data for surveillance purposes.[137]

Then there is the abuse of the privilege by the state. Heidi Swart (2017) positions this in a statement - "we as citizens have no way to effectively watch over government's use of all-seeing cyberspying technologies."[138] All democracies grapple with this social dilemma. For South Africa, the dilemma is currently quite vivid due to the state capture saga. Let us therefore consider the specifics of the SA legislative framework governing the use of social media content.

South African legislation affecting the regulation of SOCMINT

Social media is not a foreign concept to South Africa. The following statistics illustrate graphically use of the various social media applications within South Africa:

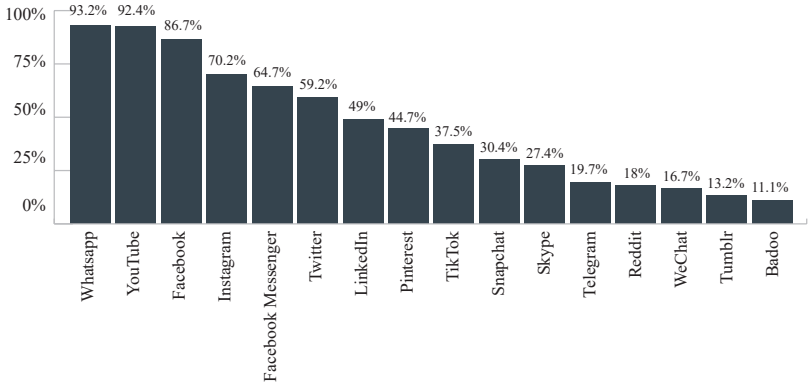

Figure 1: Most used social media platforms in South Africa, users aged 16 to 64 (mid-2021)
Source: BusinessTech (2021)[139]

Comparatively speaking, South Africa is therefore not different concerning the trends in social media usage. South Africa has also attempted regulating access to and usage of personal information available due to state and non-state organisational process requirements for registration, authentication and transparency. This does not differ from the attempts by certain European authorities and countries further afield (for example

France) to secure and guarantee privacy. Let us now review the relevant South African legislation that attempts to guarantee privacy as a constitutional right and legislation that mandate the SA intelligence services and agencies to conduct intelligence operations in national interest.

Collectively, the following legal frameworks are intent on addressing the mischief associated with the protection of information. The question is: how does this affect the state mandate to use all available social media content in terms of the SA Constitution and the Protection of Personal Information Act 4 of 2013 (the POPIA) in the interest of SA national security and security within international co-operation?

South African intelligence legislation

During (or ideally before) a national security dilemma or simply in the national interest, SA intelligence services and agencies hold legislative mandates to furnish state decision-makers with relevant and in-time intelligence. SOCMINT is one, and developing into a significant source of content that, once processed, could provide the intelligence products that could inform robust national security-related decisions. SOCMINT is also a relatively cost-effective intelligence collection method. Questions to be considered in this regard are:

- Which SA legislation affects the use of SOCMINT by SA intelligence services and agencies?
- Does SA legislation provide crisp guidance on the use of SOCMINT within the domestic national security context?
- Does the legislation also provide sanctions for transgression?

First, let us consider the SA (national security-related) intelligence mandates as legislated.

The Constitution[140] provides for the establishment of intelligence services in Chapter 11 (s 209–210): "(1) Any intelligence service, other than any intelligence division of the defence force or police service, may be established only by the President, as head of the national executive, and only in terms of national legislation."[141] The establishment of the South African State Security Agency (SSA) brought together the National Intelligence Agency (NIA) and the SA Secret Services under central command.[142] The National Strategic Intelligence Act 39 of 1994 (as amended)[143] and the Defence Act 42 of 2002 establish the respective SA intelligence services and agencies that are tasked with national security intelligence functions.

Section 2 of the National Strategic Intelligence Act 39 of 1994 describes the function of the intelligence services and agencies as to collect and process "intelligence" that would enable responses to an identified "threat or potential threat to the security of the Republic or its people".[144] The following contextual definitions of intelligence are applicable –

> "'counter-intelligence' means measures and activities conducted, instituted or taken to impede and to neutralise the effectiveness of foreign or hostile intelligence operations, to protect intelligence and any classified information, to conduct security screening investigations and to counter subversion, treason, sabotage and terrorism aimed at or against personnel, strategic installations or resources of the Republic;
>
> 'crime intelligence' means intelligence used in the prevention of crime or to conduct criminal investigations and to prepare evidence for the purpose of law enforcement and the prosecution of offenders;
>
> 'departmental intelligence' means intelligence about any threat or potential threat to the national security and stability of the Republic which falls within the functions of a department of State, and includes intelligence needed by such department in order to neutralise such a threat;
>
> 'domestic intelligence' means intelligence on any internal activity, factor or development which is detrimental to the national stability of the Republic, as well as threats or potential threats to the constitutional order of the Republic and the safety and the well-being of its people;
>
> 'national security intelligence' means intelligence which relates to or may be relevant to the assessment of any threat or potential threat to the security of the Republic in any field;
>
> 'national strategic intelligence' means comprehensive, integrated and estimative intelligence on all the current and long-term aspects of national security which are of special concern to strategic decision-making and the formulation and implementation of policy and strategy at national level."[145]

Every definition emphasises the use of intelligence for the purpose of national security threat responses within the context of state and human security paradigms, i.e., decisions, policy, strategy, planning, and others. The SSA mandate therefore relates to the provision of pre-emptive intelligence to the SA government of –

> [Any impending] domestic and foreign threats or potential threats to national stability, the constitutional order, and the safety and well-being of our people. This allows the government to implement policies to deal with potential threats and better understand existing threats, and, thus, improve their policies.[146]

The mandate for military intelligence functions is no different; it just has a particular focus on military operations with the same national aim – "'domestic military intelligence' means intelligence required for the planning and conduct of military operations within the Republic to ensure security and stability for its people".[147]

It should be noted that no detailed description of the type of intelligence is provided, i.e., the primary collection disciplines – OSINT, SIGINT, HUMINT, GEOINT, signals intelligence (SIGINT), measurement and signature intelligence (MASINT) and SOCMINT. It is assumed that all the intelligence content domains are included in the definitions above and that the state (i.e., SSA and defence intelligence) will utilise all the content from any of these domains to assess the "threats or potential threats to the constitutional order of the Republic and the safety and the well-being of its people"[148]. There is, however, other more recent legislation that needs consideration when it concerns the right to privacy as per the SA Constitution.

Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA) 70 of 2002 as amended[149]

RICA was promulgated to curb mischief that relates to the interception of communication.[150] This communication must take place on specified radio frequencies within the frequency spectrum, and RICA is positioned to regulate the telecommunication industry that does not "have the capability to be intercepted. RICA was also promulgated to regulate "certain communication-related information",[151] typically by means of the Office for Interception Centres (to be established). Thus, the intent of RICA is clear."[152] RICA would have provided the state with broad legislative cover to conduct intelligence operations within the SIGINT and SOCMINT domains. However, RICA also seeks to regulate how intelligence services and agencies go about their business. This was found wanting by the Constitutional Court, leading to the SA Constitutional Court ruling on 3 February 2021 that the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) is unconstitutional. The court argued that it did not provide "adequate safeguards to protect the right to privacy". According to BusinessTech[153], this happened after Sam Sole, a journalist who had been placed under surveillance by the SSA, challenged the constitutionality of the act. The Constitution Court believed communication interception and surveillance based on the provisions of RICA comprise a "highly invasive violation of privacy, and thus infringes on section 14 of the Constitution".[154] The court did acknowledge that state surveillance is of importance, but that the right to privacy was coupled to the right to dignity. This attests to the conceptualisation by Rønn and Søe (2019) that privacy is a cluster phenomenon, i.e., the various types of privacy invariably affect each other in an integrated manner.[155]

This Constitutional Court ruling sets a precedent for intelligence operations within the domain of SOCMINT and would typically want SOCMINT operations to be a last resort. However, not all communication is equal. When an intelligence organisation decides to intercept voice and social media communication platforms such as WhatsApp, Telegram and Twitter, it might become problematic from a 'right to privacy' perspective. These types of social media have strict password and encryption protection (informed consent controls) and can probably not be regarded as public domain or OSINT. RICA is, however, not the only SA legislation that was promulgated to regulate mischief involving the communication sector, its users and the security sector.

Protection of Personal Information Act 4 of 2013 (POPIA)[156]

The POPI Act (POPIA) has very similar wording and structure to that of the European GDPR. The mischief that the POPIA (section 1) is endeavouring to regulate comprises infringements on the right to privacy, the flow of information domestically and "across international borders", lawful processing of personal information, and recourse where this was infringed upon.[157] POPIA (section 4) provides the parameters for the lawful use of personal information. Typically, principles of accountability, openness, quality safeguards, limitations for processing, and participation of the individual are addressed and then dealt with and addressed in various other sections of the POPIA.[158]

The rights of everyone in terms of personal information and exclusion are addressed in POPIA (sections 5 and 6). Without being trapped in a discussion about what the individual rights to privacy are, let us focus on what is excluded by the POPIA. Section 6 addresses exclusions of particular importance. Within the context of this article, these are reflected in section 6(1)(c)(i) –

> 6. (1) This Act does not apply to the processing of personal information – (c) by or on behalf of a public body – (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or (ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information.[159]

A specific calibration of this exclusion for national security purposes is section 6(2), which points the reader to the Protection of Constitutional Democracy against Terrorist and Related Activities Act 33 of 2004 (section 4), "Terrorist and related activities".

The POPIA (section 7) refers to the "Exclusion for journalistic, literary or artistic purposes", which is also outside the discussion about SOCMINT and intelligence organisations and their operational needs. However, with the exclusions expressed in POPIA (section 7), another channel of access to SOCMINT is opened to intelligence organisations that are experts in HUMINT collection. It is also common knowledge that some of the most capable intelligence organisations have journalism as their core business. Partnerships between intelligence organisations and media organisations are common.

From an SA perspective, personal information disclosed and distributed via social media is in the public domain, but that does not automatically render such information free to use. That use is regulated by the POPIA.[160] The state, however, retains the right to access and process personal information – including social media content – for the purpose of securing the nation against specified national security threats.[161,162] The only caveat is that the SA intelligence services and agencies are responsible for the promulgation of

departmental regulations – or "adequate safeguards"[163] – to prevent the abuse of this privilege extended by POPIA. The effectivity of such regulations (if in existence) has not yet been tested in court.

Criminal Procedures Act 51 of 1977 (as amended)

The relevance of the Criminal Procedures Act[164] is in the authorisation of surveillance of individuals. This includes the surveillance of individual social media accounts. It thus remains an issue of the right to privacy and whether that right carries more weight than the 'wellbeing of the nation' from a national security threat perspective.

Recommendations

Omand offers two approaches to the implementation of SOCMINT regulation. One avenue would be with 'open SOCMINT', which is characteristically non-intrusive in nature due to the requirement for consent to access any social media account[165]. If such consent cannot be secured, further use of any account content becomes restricted from a privacy perspective.[166] There is thus a reasonable expectation by the user that private content will remain just that. Content that is collected by 'open SOCMINT' is therefore essentially OSINT, and organisations that collect such content should be expected to be, from a UK perspective –

> [As] transparent as possible that:
>
> - all such collection, retention, and sharing policies are publicised and justified
> - the reason why the information is collected is publicised
> - the information commissioner should monitor the development
>
> of this form of information processing to ensure that it conforms with the principles of the Data Protection Act [2018], including being fairly and lawfully processed in accordance with individuals' rights.[167]

The second avenue could be with "intrusive interception and surveillance" [168]. The first avenue does not seem to pose much challenge in terms of regulation, and essentially refers to OSINT. However, the second avenue is the approach that separates SOCMINT from OSINT. For this avenue to be institutionalised in legislation and departmental policy, Omand (2012) envisages six principles, providing a first-order regulatory foundation for SOCMINT collection and exploitation:

> [1] [T]here must be sufficient, sustainable cause; [2] there must be integrity of motive; [3] the methods used must be proportionate and necessary; [4] there must be right authority, validated by external oversight; [5] recourse to secret intelligence must be a last resort if more open sources can be used; [and 6] there must be reasonable prospect of success.[169]

Principle 5, alluding to the use of SOCMINT as a last resort, is counter-productive. Because social media is currently (and will be in future) the first choice for communication

it would be prudent for intelligence services and agencies to make SOCMINT their first port of call.

Somewhere between the need for privacy and national security there consequently should be a Venn diagram moment that provides space for the articulation of policy recommendations that protect the user from the state and the state from the user. Lever (2016) [170], Rønn and Søe (2019)[171] and others conceptualised some nuanced arguments about the privacy–security nexus. Lever (2016) argues from the perspective of democratic rule that states must have the ability to "hold associations to account for their actions" [172], merging the right to privacy and the mandate to provide security into a requirement for operational freedom within the limits set by legislation (which invariably will be based on issues of ethics, morality, rights and freedoms). She further states:

> Constraints on privacy are necessary to protect 'the rule of law', because we cannot form, pass, judge and execute laws democratically without devices such as the secret ballot, or legal rights of confidential judgement, information and association, which enable people carefully to explore alone, and with others they know and trust, what they should do as citizens. Our legitimate interests in privacy are not negligible, or inherently of lesser importance than our interests in security.[173]

This is further calibrated by the contention that individual "interests in privacy, then, can be varied and inescapably tied to our sense of ourselves as moral agents. They are not, therefore of obviously lesser importance than our interests in self-preservation – individual, or collective".[174] "Public acceptability lies at the heart of any form of intelligence collection, and this can only be secured if SOCMINT is properly used and properly authorized."[175] SOCMINT and OSINT should therefore be separate collection domains to protect the imperative of the right to privacy and national security requirements better and in a balanced manner by means of unambiguous national regulation in the interest of the citizen.

Conclusion

South Africa is a very large producer, distributer and consumer of social media content from both a public and a state intelligence perspective. Intelligence services can benefit – and are probably already benefitting – from the use and exploitation of SOCMINT. However, there is a growing concern from the public about the negative consequences that such collection and exploitation could have on an individual's right to privacy. This is also an international concern.

Given the legal complexities of SOCMINT, it is proposed that SOCMINT should be viewed as a new collection discipline, and South Africa should embark on a process to provide clear legislative guidelines for the collection and exploitation of SOCMINT. South Africa is (at present) still in the unique position to use SOCMINT and could use SOCMINT in intelligence collaboration with international partners that do not have that liberty. Due regard should be exercised in this regard because of the effect such sharing might have on possible international relations.

From a state mandate perspective, SA intelligence services and agencies are clearly mandated within several distinct pieces of legislation to conduct all aspects of intelligence domestically and in foreign locations. Considering the existence and acceptance of SOCMINT, as a 'relatively new' phenomenon when compared to the rest of the primary collection disciplines (OSINT, SIGINT, HUMINT, GEOINT, MASINT), SA intelligence services and agencies are permitted to mine and exploit social media content to produce SOCMINT for the purpose of decision-making within the context of national security. Such actions are calibrated by specifications in the POPIA.

Grounded in the fact that the SOCMINT content volume is considerable and expanding exponentially, South Africa should establish, within its respective intelligence services and agencies that specifically manage collection and exploitation of SOCMINT, policy guidelines for the use of SOCMINT that distinguish between what can be defined as OSINT and what is quintessentially SOCMINT. It would also be incumbent on these organisations to ensure that robust construct definitions are included in departmental policy, stipulating the differences in requirements for the legal usage of OSINT vs SOCMINT. Those differences do exist and should be formalised post haste. Recommended in this regard is that SOCMINT be conceptualised and institutionalised in departmental policy as the product of privileged (i.e., access authorisation required) social media content analysis, whereas OSINT is the product of analysed public content (i.e., no access authority required). The primary difference is locked into the legislated imperatives of privacy versus national security; hence, the SOCMINT–OSINT nexus.

Consideration should be given to govern the collection and exploitation of SOCMINT by means of (possibly) several operating principles that ensure maximum protection of privacy without eroding the mandate of the state to ensure national security. Such principles could include requirements for a clear legal case showing cause and evidence of operational response proportionality. These issues should be in an executive order (the format of which could be described in legislation) to ensure boundary management and oversight. As with requirements for covert action operations, a successful conclusion of the operation should be achievable with clear consequences spelled out if the operation fails.

ENDNOTES

[67] K Alspach. "Going on offense: Ukraine forms an 'IT army', Nvidia hacks back". *Venturebeat.* 26 February 022. <https://venturebeat.com/2022/02/26/going-on-offense-ukraine-forms-an-it-army-nvidia-hacks-back/> Accessed on 15 January 2022.

[68] *The Conversation*. "Guns, tanks and Twitter: How Russia and Ukraine are using social media as the war drags on". 5 April 2022. <https://theconversation.com/guns-tanks-and-twitter-how-russia-and-ukraine-are-using-social-media-as-the-war-drags-on-180131> Accessed on 18 April 2022. There is a wealth of such content available on the World Wide Web.

[69] JI Stegen. "Social media intelligence (SOCMINT) within the South African context: A theoretical and strategic framework for the national security environment". PhD dissertation. North-West University, 2019, 194. <orcid.org 0000-0002-8420-999X> Accessed on 15 January 2022.

[70] Schram (2018) and Cohn (2011), cited in *Ibid*., p. 194.

[71] Schram (2018) and Mayfield (2008), cited in *Ibid*.

[72] D Omand, J Bartlett & C Miller. "Introducing social media intelligence (SOCMINT)". *Intelligence & National Security* 27/6. 2012. 801–823. doi: 10.1080/02684527.2012.716965

[73] *Britannica*. 2021. "Internet – computer network". <https://www.britannica.com/technology/Internet> Accessed on 17 January 2022.

[74] *Ibid*.

[75] MY Abuhashesh, H Al-Dmour, RE Masa'deh, A Salman, R Al-Dmour, M Boguszewicz-Kreft & QN Alamaireh. "The role of social media in raising public health awareness during the pandemic COVID-19: An international comparative study". *Informatics* 80. 2021. 1-19.

[76] R Momi. 2021. "SOCMINT: Social media intelligence a new discipline?" *Tradecraft.* 12 November 2021. <https://www.greydynamics.com/socmint-social-media-intelligence-a-new-discipline/> Accessed on 18 April 2022. Perspectives of Omand et al. op. cit., p. 801 is discussed.

[77] Omand *et al. op. cit*., p. 801.

[78] "Arab Spring, wave of pro-democracy protests and uprisings that took place in the Middle East and North Africa beginning in 2010 and 2011, challenging some of the region's entrenched authoritarian regimes. The wave began when protests in Tunisia and Egypt toppled their regimes in quick succession, inspiring similar attempts in other Arab countries. Not every country saw success in the protest movement, however, and demonstrators expressing their political and economic grievances were often met with violent crackdowns by their countries' security forces. For detailed coverage of the Arab Spring in individual countries, *see* Jasmine Revolution (Tunisia), Egypt Uprising of 2011, Yemen Uprising of 2011–12, Libya Revolt of 2011, and Syrian Civil War." Britannica. 2021. "Arab Spring - pro-democracy protests". <https://www.britannica.com/event/Arab-Spring> Accessed on 16 May 2022.

[79] G Wolfsfeld, E Segev & T Sheafer. "Social media and the Arab Spring: Politics comes first". *The International Journal of Press/Politics* 18/2. 2013. 115–137. doi: 10.1177/1940161212471716.

[80] BA Senekal. "SOCMINT: The monitoring of social media for community safety purposes within a big data framework in South Africa with specific reference to Orania". *Litnet.* 14 November 2018. <https://www.litnet.co.za/socmint-the-monitoring-of-social-media-for-community-safety-purposes-within-a-big-data-framework-in-south-africa-with-specific-reference-to-orania/> Accessed on 18 April 2022.

[81] H Brown, E Guskin & A Mitchell. "The role of social media in the Arab uprisings". Pew Research Centre. 28 November 2012. <https://www.pewresearch.org/journalism/2012/11/28/role-social-media-arab-uprisings/> Accessed on 17 January 2022.

[82] *Ibid*.

[83] *Ibid*.

[84] A Smidi & S Shahin. "Social media and social mobilisation in the Middle East". *India Quarterly* 73/2. 2017. 196–209.

[85] NA Hassan. "A guide to social media intelligence gathering (SOCMINT)". Secjuice. 21 June 2020. <https://www.secjuice.com/social-media-intelligence-socmint/> Accessed on 17 January 2022.

[86] KT Davis. "SOCMINT: The cutting edge of the invisible line". Master's thesis. American Public University System, 2015. <https://www.academia.edu/30921500/SOCMINT_THE_CUTTING_EDGE_OF_THE_INVISIBLE_LINE?auto=download> Accessed on 18 April 2022.

[87] H Swart. "Government surveillance of social media is rife: Guess who's selling your data?" *Daily Maverick*. 25 April 2018. <https://www.dailymaverick.co.za/article/2018-04-25-government-surveillance-of-social-media-is-rife-guess-whos-selling-your-data/#:~:text=And%20that%20includes%20the%20South,to%20release%20your%20private%20data.&text=Ultimately%2C%20the%20state%20can%20use,right%20up%20to%20your%20door> Accessed on 14 January 2022.

[88] MM Lowenthal & RM Clark. *The five disciplines of intelligence collection*. Los Angeles: Sage, 2015.

[89] T Constantin-Sorin. "Social media intelligence". Perconcordiam.com. 2019. <https://perconcordiam.com/social-media-intelligence/> Accessed on 20 January 2022.

[90] Momi *op. cit.*

[91] Constantin-Sorin *op. cit*.

[92] IA Ivan, IC Anamaria, LR Codruta & GM Nicolae. "Social media intelligence: Opportunities and limitations". CES working papers. Massachusetts: Centre for European Studies, Alexandru Ioan Cuza University of Iasi, 2015, 506. See also R Norton-Taylor. "Former spy chief calls for laws on online snooping". *The Guardian.* 24 April 2012. <http://www.theguardian.com/technology/2012/apr/24/former-spy-chieflaws-Snooping> Accessed on 30 May 2014.

[93] Lowenthal & Clark *op. cit*.

[94] KT Davis. "SOCMINT: The cutting edge of the invisible line". Master's thesis. American Public University System, 2015

[95] Ivan, Anamaria, Codruta & Nicolae *op cit.*

[96] T Constantin-Sorin. "Social Media Intelligence By Using Facebook, Twitter and other sites to combat organized crime". per Cordium, Journal of European Security and Defense Issues, 9(4). 2019. 18-23.

[97] Privacy International. "Social media intelligence". 23 October 2017. <https://privacyinternational.org/explainer/55/social-media-intelligence#:~:text=Social%20media%20intelligence%20(SOCMINT)%20refers,such%20as%20Facebook%20or%20Twitter> Accessed on 18 April 2022.

[98] KV Rønn & SO Søe. "Is social media intelligence private? Privacy in public and the nature of social media intelligence". *Intelligence and National Security* 34/3. 2019. 363.

[99] *Ibid*., 363.

100 Tavani, "Informational Privacy"; DeCew, Privacy; and Solove, Understanding Privacy in Rønn & Søe *op cit*.

[101] Rønn & Søe *op cit,* p. 363.

[102] Rønn & Søe *op cit,* p. 363.

[103] D Mercer & A Culbertson. "Five minutes of terror: How the London Bridge attack unfolded". *Sky News.* 4 June 2021. <https://news.sky.com/story/how-the-london-bridge-terror-attack-unfolded-11874155> Accessed on 17 April 2022.

[104] Rønn & Søe *op. cit*., p. 374.

[105] *Ibid*., p. 374.

[106] *Ibid*., p. 365.

[107] *Ibid*. Discussed on pp. 365, 369, 370 and 374.

[108] *Ibid*., p.365.

[109] DataReportal. 2022. "Facebook stats and trends". <https://datareportal.com/essential-facebook-stats#:~:text=Here's%20what%20the%20latest%20data,)%3A%20 2.910%20billion%20(October%202021)&text=Number%20of%20people%20 who%20use,)%3A%201.930%20billion%20(October%202021)&text=Share%20 of%20Facebook's%20monthly%20active,%3A%2066%25%20(October%202021)> Accessed on 19 January 2021.

[110] *Ibid*.

[111] P Caddick-Adams. "The fascinating story of how ordinary Brits' holiday postcards helped win D-Day". *The Sun.* 6 June 2019. <https://www.thesun.co.uk/news/9229653/d-day-british-postcards-helped-win/> Accessed on 19 January 2022.

[112] *Ibid*.

[113] C Smith. "Facebook users are uploading 350 million new photos each day". *Business Insider.* 18 September 2013. <https://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9?IR=T> Accessed on 17 January 2022.

[114] TJ Thomson, D Angus & P Dootson. "3.2 billion images and 720,000 hours of video are shared online daily. Can you sort real from fake?" *The Conversation.* 3 November 2020. <https://theconversation.com/3-2-billion-images-and-720-000-hours-of-video-are-shared-online-daily-can-you-sort-real-from-fake-148630> Accessed on 17 January 2022.

[115] D Omand, J Bartlett & M Miller. 2013. "#Intelligence". DEMOS. 2012, 9. <http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327> Accessed on 18 April 2022; Davis *op. cit*.

[116] Swart "Government surveillance …" *op. cit*.

[117] Facebook Help Centre. "What categories of my Facebook data are available to me?" <https://web.facebook.com/help/405183566203254?_rdc=1&_rdr> Accessed on 22 January 2022.

[118] A Golts. "The Russian Army to be subordinated to the National Guard in a crisis". *Eurasia Daily Monitor* 14/76. 2017. <https://jamestown.org/program/russian-army-subordinated-national-guard-crisis/> Accessed on 17 January 2022.

[119] *Ibid*.

[120] P Fabricius. "Pretoria's contortions in trying to maintain some sort of neutrality on Russia's invasion of SA's egg dance on war in Europe a lesson in how not to win friends and influence people". *Daily Maverick.* 26 March 2022. <https://www.dailymaverick.co.za/article/2022-03-26-sas-egg-dance-on-war-in-europe-a-lesson-in-how-not-to-win-friends-and-influence-people/> Accessed on 18 April 2022.

[121] N Kobie. "The complicated truth about China's social credit system". *Wired.* 7 June 2019. <https://www.wired.co.uk/article/china-social-credit-system-explained> Accessed on 17 January 2022.

[122] GH Barbier & R Goolsby. "Harnessing the crowdsourcing power of social media for disaster relief". *IEEE Intelligent Systems* 26/3. 2011. 10–14.
[123] A Hunt & D Specht. "Crowdsourced mapping in crisis zones: Collaboration, organisation and impact". *Journal of International Humanitarian Action* 4/1. 2019. doi: 10.1186/s41018-018-0048-1ht
[124] Stegen *op. cit*., p. 195.
[125] Z Bauman. *Liquid modernity*. Cambridge: Polity Press, 2006.
[126] Stegen, *op cit*.
[127] Wolfsfeld *et al. op. cit*.
[128] NA Hassan. "A guide to social media intelligence gathering (SOCMINT)". Secjuice. 21 June 2020. <https://www.secjuice.com/social-media-intelligence-socmint/> Accessed on 17 January 2022
[129] For quick access to the General Data Protection Regulation (GDPR) the following webaddress is suggested <https://gdpr-info.eu/> Accessed on 26 January 2022.
[130] B Wolford. "What is GDPR, the EU's new data protection law?" GDPR.EU. 2021. <https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU> Accessed on 17 January 2022.
[131] *Ibid*.
[132] *Ibid*.
[133] *Ibid*.
[134] *Ibid*.
[135] *Ibid*.
[136] Swart "Government surveillance …" *op. cit*.
[137] *Ibid*.
[138] H Swart. "Cyberspying: The Ghost in Your Machine". < https://www.dailymaverick.co.za/article/2017-02-21-cyberspying-the-ghost-in-your-machine/> Accessed on 17 January 2022. Also refer to H Swart. "Social media surveillance may not just be urban legend". Daily Maverick. 20 October 2017. <https://www.dailymaverick.co.za/article/2017-10-20-op-ed-social-media-surveillance-may-not-just-be-urban-legend/#> Accessed on 17 January 2022.
[139] BusinessTech. "The biggest and most popular social media platforms in South Africa, including TikTok". *BusinessTech*, 1 July 2021. <https://businesstech.co.za/news/internet/502583/the-biggest-and-most-popular-social-media-platforms-in-south-africa-including-tiktok/> Accessed on 18 May 2022.
[140] Constitution of the Republic of South Africa, 1996.
[141] *Ibid*., Chapter 11, Section 209–210.
[142] *Polity*. "National Strategic Intelligence Act (No. 67 of 2002)". 2022. <https://www.polity.org.za/article/national-strategic-intelligence-act-no-67-of-2002-2002-01-01> Accessed on 17 January 2022.
[143] "To amend the National Strategic Intelligence Act, 1994 so as to exclude the Minister as a member of Nicoc; to redefine counter-intelligence; to provide for security screening by the relevant members of the national intelligence structures; to further define the functions of the Minister pertaining to co-ordination of intelligence: and to regulate the functions of the National Intelligence Structures; and to provide for matters connected therewith" (*Ibid*.).
[144] South African Government. "National Strategic Intelligence Act 39 of 1994". 1994, Section 2(1)(b)(i). <https://www.gov.za/documents/national-strategic-intelligence-act> Accessed on 22 January 2022.
[145] *Ibid*., Section 1.
[146] National Government of South Africa. "State Security Agency (SSA)". 2022 <https://nationalgovernment.co.za/units/view/42/state-security-agency-ssa> Accessed on 17 January 2022.

[147] Republic of South Africa. "Defence Act No. 42 of 2002". *Government Gazette* 452/24576. 2002. Chapter 6, Section 32. <https://www.gov.za/sites/default/files/gcis_document/201409/a42-020.pdf> Accessed on 17 January 2022.

[148] Republic of South Africa. "State Security Agency (SSA) – Overview." https://nationalgovernment.co.za/units/view/42/state-security-agency-ssa> Accessed on 17 January 2022.

[149] Republic of South Africa. "Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002". *Government Gazette* 451/24286. 2002. <https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf> Accessed on 13 January 2022.

[150] "'[C]ommunication' includes both a direct communication and an indirect communication" (*Ibid*.).

[151] "'[C]ommunication-related information' means any information relating to an indirect communication which is available in the records of a telecommunication service provider, and includes switching, dialling or signalling information that identities the origin, destination, termination, duration, and equipment used in respect of each indirect communication generated or received by a customer or user of any equipment, facility or service prohibited by such a telecommunication service provider and, where applicable, the location of the user within the telecommunication system" (*Ibid*.).

[152] Republic of South Africa, "Regulation of Interception …" *op. cit*.

[153] *BusinessTech*. "South Africa's RICA law is unconstitutional: Court ruling". *BusinessTech*, 4 February 2021. <https://businesstech.co.za/news/technology/465518/south-africas-rica-law-is-unconstitutional/#:~:text=South%20Africa's%20Constitutional%20Court%20has,Act%20(RICA)%20is%20unconstitutional> Accessed on 17 January 2022.

[154] *Ibid*.

[155] Rønn & Søe *op. cit*., p. 364.

[156] "It was 1 July 2020 and the one year grace period to comply ended on 30 June 2021. Parliament assented to POPIA on 19 November 2013. The commencement date of section 1, Part A of Chapter 5, section 112 and section 113 was 11 April 2014. The commencement date of the other sections was 1 July 2020 (except for section 110 and 114(4). The President of South Africa has proclaimed the POPI commencement date to be 1 July 2020." Accessible Law. "Protection of Personal Information Act (POPI Act)". 2022. <https://popia.co.za/> Accessed on 17 January 2022.

[157] Republic of South Africa. "Protection of Personal Information Act No. 4 of 2013". *Government Gazette* 581/37067. 2013. 16. <https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf> Accessed on 17 January 2022.

[158] *Ibid*., p. 19.

[159] *Ibid*., pp. 21–22.

[160] Swart, "Government surveillance …" *op cit.*

[161] *Ibid*.

[162] Republic of South Africa. "Protection of Personal Information Act …" *op. cit*., pp. 21–22.

[163] *Ibid*., p. 22.

[164] Department of Justice and Constitutional Development. "Criminal Procedure Act 51 of 1977". <https://www.justice.gov.za/legislation/acts/1977-051.pdf> Accessed on 28 January 2022.

[165] D Omand, J Bartlett & C Miller. "A balance between security and privacy online must be struck…" #INTELLIGENCE," London: Demos, 2012, 38.

[166] *Ibid*., 38.

[167] *Ibid*., pp. 39–40. Also see Omand *et al. op. cit.* for a more detailed discussion on access, legitimacy, process and other important distinguishing features of SOCMINT.
[168] *Ibid*., pp. 40.
[169] Omand *op. cit.* Also see Omand *et al*., "#Intelligence" *op. cit.*; Davis *op. cit*.
[170] A Lever. "Democracy, privacy and security". In AD Moore, ed, *Privacy, security and accountability.* Rowman & Littlefield, 2016, 13. <https://hal-sciencespo.archives-ouvertes.fr/hal-02506502/document> Accessed on 18 April 2022.
[171] Rønn & Søe *op cit*.
[172] Lever *op cit.*
[173] Lever *op cit*.
[174] Lever *op cit*, p. 14.
[175] Omand *et al*., "Introducing social media intelligence …" *op. cit*., p. 802.