THE RIGHT TO PRIVACY IN THE DIGITAL AGE: RECENT DEVELOPMENTS AND CHALLENGES

Dr. Alecia Johns, DPhil (Oxon.)
Simmonds Building
30 DeCastro Street
Road Town, Tortola
British Virgin Islands
Phone : +1 (284) 494-5808
ajohns@onealwebster.com

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

STEP Caribbean Conference, St. Lucia April 25 – 27, 2016

INTRODUCTION

The right to privacy has long been considered a fundamental human right and is widely recognised in numerous regional and international human rights instruments. For example, Article 12 of the 1948 Universal Declaration of Human Rights provides that, 'No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks upon his honour and reputation'. The importance of the right to privacy stems from the fact that it remains necessary for the effective enjoyment of many other rights and freedoms,[1] given that it enables the individual to define the parameters of his personal sphere which he or she enjoys and navigates free from social and governmental encroachment. This is essential for the full realisation of, among other things, the freedoms of expression and association. In light of this, many Bills of Rights articulate freedom of expression as necessarily including freedom from interference with one's correspondence.[2]

Notwithstanding the importance of the right to privacy, it is by no means absolute. It is a qualified right which may usually be limited in the interests of public safety, national security, or the protection of the rights and freedoms of others. These necessary qualifications give rise to a perpetual tension between the citizen's right to privacy and the state's responsibility for the maintenance of safety and security. With the increasing storage and transmission of data and communication electronically, new challenges arise regarding the protection of the individual's right to privacy given the enhanced vulnerability stemming from the threats of interception and surveillance in the digital age. This paper briefly outlines some of the recent developments and challenges in this area, with a specific focus on the implications of these developments within the Caribbean regional context.

[1] As noted by Voilo, 'In one sense all human rights are aspects of the right to privacy.' See Fernando Volio, "Legal Personality, Privacy and the Family" in Henkin (ed) *The International Bill of Rights* (Colombia University Press 1981).

[2] See Figure 1 below.

THE GENERAL NATURE AND SCOPE OF THE RIGHT TO PRIVACY

The right to privacy was defined by Brandeis and Warren in 1890 as 'the right to be left alone'.[3] This right has since come to encompass many facets,[4] including but not limited to:

- *Informational Privacy*: which involves freedom from unlawful interference with one's personal data.[5]
- *Bodily Privacy*: which concerns the protection of people's physical bodies from invasive procedures and practices.
- *Privacy of communications*: this includes the security and privacy of mail, telephones, email and other communication.
- *Territorial Privacy*: which concerns setting limits on the intrusion of an individual's home and other property.

The Right to Privacy in International and Regional Human Rights Law

As noted above, a number of regional and international human rights instruments include the right to privacy, normally expressed with emphasis on communications and territorial privacy in the wording of a prohibition against interference with one's 'privacy, family, home or correspondence'.[6] Article 8 of the European Convention on Human Rights (ECHR) similarly provides the following:

"Everyone has the right to respect for his private and family life, his home and his correspondence."

The European Court of Human Rights (the ECtHR) has interpreted the scope of this provision very broadly, holding that private life is incapable of exhaustive definition and may even include activities of a professional or business nature.[7] Private life has been taken to include the choice of affirming and assuming one's sexual identity, with the result that legislation criminalising homosexual conduct was held to unjustifiably interfere with the right to private life under Article 8.[8] The ECtHR

[3] Samuel Warren and Louis Brandeis, "The Right to Privacy" (1890) 4(5) Harvard Law Review 193.

[4] See Global Internet Liberty Campaign, "Privacy and Human Rights: An International Survey of Privacy Laws and Practice" (1997) <http://gilc.org/privacy/survey/intro.html>

[5] See *X v United Kingdom* App no 9072/82 (ECHR, 6 October 1982); *Murray v United Kingdom* Series A No. 300-A (ECHR, 28 October 1994); *Leander v Sweden* Series A No. 116 (ECHR, 26 March 1987); *MK v France* App no 19522/09 (ECHR, 18 April 2013).

[6] International Covenant on Civil and Political Rights, Article 17; American Convention on Human Rights, Article 11; UN Convention on the Rights of the Child, Article 16; Arab Charter on Human Rights, Article 21.

[7] *Niemietz v Germany* Series A no. 251-B (ECHR, 16 December 1992); *Halford v the United Kingdom*, *Reports* 1997-III (ECHR, 25 June 1997).

[8] *Dudgeon v United Kingdom* App no 7525/76 (ECHR, 22 October 1981).

also recognised the right as including bodily privacy on the basis that private life covers 'the physical and moral integrity of the person'.[9]

The ECtHR has also, vey importantly, firmly established the primacy of informational and communications privacy with the effect that a strong foundation exists for the protection of personal data and online privacy in the face of ever-changing technologies. The Court has held that article 8 has been infringed in cases of wire-tapping of telephone conversations,[10] as well as mass surveillance of email correspondence.[11] It has also been held that the systematic storage and collection of personal data by security services in the absence of certain minimum legal safeguards violates the citizen's right to privacy under article 8.[12]

One emerging area of interest regarding informational privacy, is whether certain tax reporting obligations, such as those under the OECD's Common Reporting Standard (CRS) may be held to be in contravention with article 8 of the ECHR.[13] CRS allows for a global automatic exchange of taxpayers' financial account information to tax authorities in their country of residence via an IT platform.[14] Legitimate concerns have been raised about the proportionality and ultimate security of such indiscriminate automatic exchanges and it remains to be seen whether a successful challenge may be mounted on the basis of article 8.[15]

The Right to Privacy in Caribbean Constitutions

The constitutions of most Caribbean states include some recognition of the individual's right to privacy, albeit to varying degrees and in various forms. The right is often addressed in one or more of the following ways:

---

[9] *X & Y v Netherlands* App no 8978/80 (ECHR, 26 March 1985) para 22; *Costello-Roberts v United Kingdom* App no 13134/87 (ECHR, 25 March 1993) para 36.

[10] *A v France* App no 14838/89 (ECHR, 23 November 1993); *Halford v United Kingdom*, supra n 7.

[11] *Liberty v UK* App no 58243/00 (ECHR, 1 July 2008); See also *Copland v United Kingdom* App No 62617/00 (ECHR, 3 April 2007) where the Court held that metadata, relating to the location, source and timing of communications (but excluding their content), also fell within the scope of 'correspondence' under Article 8.

[12] *Shimovolos v Russia* App no 30194/09 (ECHR, 21 June 2011).

[13] See Filippo Noseda, 'Trusts and Privacy: A new battle front' <http://reaction.withersworldwide.com/reaction/pdfs/TrustsAndPrivacyANewBattleFront.pdf>

[14] For more on CRS see: Vanessa King and Alecia Johns, 'BVI adopts OECD's Common Reporting Standard for financial institutions' <http://onealwebster.com/bvi-adopts-oecds-common-reporting-standard-for-financial-institutions/>

[15] Noseda, supra n 13; see also Filippo Noseda, 'Erosion of the Right to Keep our Finances Private is a Step too Far' *Financial Times* (21 March 2016).

- An Express Right to Privacy;
- Freedom from interference with correspondence;
- Protection from Arbitrary Search of Property (Territorial Privacy); and
- Reference to the protection of privacy in the Preamble to the Bill of Rights.

Figure 1, below, summarises the extent of recognition in the constitutions of selected Caribbean states:

Jurisdiction	Express Right to Privacy	Freedom from Interference with Correspondence	Protection from Unlawful Property Search	Preamble Reference
Anguilla		✓ Sec 11(1)	✓ Sec 8	✓ Sec 1
Antigua		✓ Sec 12(1)	✓ Sec 10(1)	✓ Sec 3
Bahamas		✓ Art 23(1)	✓ Art 21	✓ Art 15
Barbados		✓ Sec 20(1)	✓ Sec 17	✓ Sec 11(b)
Belize	✓ Sec 14(1)	✓ Sec 12(1)	✓ Sec 9	✓ Sec 3(c)
British Virgin Islands	✓ Sec 19(1)	✓ Sec 23(2)	✓ Sec 19(2)	✓ Sec 9(c)
Cayman Islands	✓ Sec 9(1)	✓ Sec 11(1)	✓ Sec 9(2)	
Dominica		✓ Sec 10(1)	✓ Sec 7(1)	✓ Sec 1(c)
Grenada		✓ Sec 10(1)	✓ Sec 7	✓ Sec 1(c)
Guyana		✓ Sec 146(1)	✓ Sec 143	✓ Sec 40(1)(c)
Jamaica	✓ Sec 13(3)(j)	✓ Sec 13(3)(j)	✓ Sec 13(3)(j)	
St. Kitts		✓ Sec 12(1)	✓ Sec 9(1)	✓ Sec 3(c)
St. Lucia		✓ Sec 10(1)	✓ Sec 7(1)	✓ Sec 1(c)
St. Vincent		✓ Sec 10(1)	✓ Sec 7(1)	✓ Sec 1(c)
Trinidad and Tobago	✓ Sec 4(c)			
Turks and Caicos	✓ Sec 9(1)	✓ Sec 13(1)	✓ Sec 9(1)	✓ Sec 1(c)

Figure 1: Recognition of Privacy Rights in Caribbean Constitutions

As evidenced in Figure 1, most constitutions do not include an express right to privacy in general terms. Those which do tend to be newer provisions which were passed or amended within the last ten years.[16] Given the many facets of the right to privacy, the inclusion of an express, free-standing right offers the greatest protection against abuses of informational and communications privacy in the digital age.

Notwithstanding, it is noteworthy that communications privacy may still be adequately protected in most constitutions given the presence of a right to 'freedom from interference with correspondence'. In the 2014 Privy Council decision of *Newbold v Commissioner of Police*,[17] on appeal from the Bahamas, the Board considered whether article 23 of the Bahamas Constitution, which guarantees freedom from interference with correspondence, necessarily covered telephone interception. The Privy Council held that it did. This was on the basis that the enjoyment of one's free expression is inhibited by the consciousness that what is expressed may be the subject of unregulated surveillance.[18] Constitutions which provide for a general freedom from interference with correspondence therefore theoretically possess an added layer of protection against the threat of online surveillance. However, such provisions may still not necessarily cover informational privacy regarding the electronic use and distribution of one's personal data, in circumstances where communications or correspondence are not directly interfered with.

Regarding the right to protection from arbitrary property search, the court in *Newbold* took a much narrower approach. It held that this provision could not be said to encompass the interception of telephone conversations, given that the drafting history of the provision spoke against such a broad interpretation; the provision was held to be limited to the unlawful search of and entry on property and premises.[19] On the Board's view, such territorial privacy rights would not therefore bear relevance to the protection of privacy in the electronic context.

The final mode of recognition is the reference in most preambles to "protection for the privacy of one's home and other property." While this may be thought to guarantee a general right to privacy, the efficacy of such provisions is greatly undermined by the fact that preambles have generally been held to be unenforceable, given that they are merely introducing subsequently conferred rights and

[16] Jamaica (2011); Turks and Caicos (2011); Cayman Islands (2009); British Virgin Islands (2007); Exceptions to this are: Belize (1981) and Trinidad and Tobago (1976).

[17] (2014) 84 WIR 8; [2014] UKPC 12.

[18] *Newbold*, paras 25 – 26.

[19] *Newbold*, paras 22 – 24.

are not themselves considered to be the source of any freestanding rights.[20] By way of example, article 15 of the Bahamas Constitution provides the following:

> *"Whereas every person in The Bahamas is entitled to the fundamental rights and freedoms of the individual, that is to say, has the right, whatever his race, place of origin, political opinions, colour, creed or sex, but subject to respect for the rights and freedoms of others and for the public interest, to each and all of the following, namely-*
>
> (a) life, liberty, security of the person and the protection of the law;
>
> (b) freedom of conscience, of expression and of assembly and association; and
>
> (c) **protection for the privacy of his home and other property** and
>
> *from deprivation of property without compensation, the subsequent provisions of this Chapter shall have effect for the purpose of affording protection to the aforesaid rights and freedoms subject to such limitations of that protection as are contained in those provisions, being limitations designed to ensure that the enjoyment of the said rights and freedoms by any individual does not prejudice the rights and freedoms of others or the public interest." (Emphasis Added)*

Similarly-worded preambles are included in a number of other Caribbean constitutions.[21] In the *Newbold* case, the appellant sought to argue that article 15 of the Bahamas constitution conferred a free-standing right to privacy which was not subject to the constitution's savings law clause. The Privy Council rejected this argument and distinguished a number of earlier cases which may have been interpreted as trending towards the enforceability of preambles.[22] The prevailing position in more recent decisions is that introductory preambles of the kind referenced above do not confer separately enforceable constitutional rights.[23] This is significant for territories which lack an express right to privacy, but which include such preambular recognition. The upshot is that the preamble offers no added, enforceable protection of an individual's privacy rights. Reliance must therefore be had on other provisions which only specifically safeguard communications and territorial privacy. A gap therefore exists in many regional constitutions which lack adequate recognition and protection of information and data privacy in the Internet age.

---

[20] See *AG of Anguilla v Lake* Civil Appeal no 4 of 2004 (Eastern Caribbean Court of Appeal, 4 April 2005); *Grape Bay Ltd v AG of Bermuda* [2000] 1 WLR 574; *Campbell-Rodriques and others v AG of Jamaica* [2007] UKPC 65.

[21] See Figure 1, column 5.

[22] These cases include: *Thomas v Baptiste* (1999) 54 WIR 387; *Neville Lewis v AG* (2000) 57 WIR 275; *AG of Barbados v Boyce & Joseph* (2006) 69 WIR 104. (See paras 28 to 33 of the *Newbold* judgment).

[23] *Campbell-Rodriques*, supra n 20; *Newbold*, supra n 17.

THE RIGHT TO PRIVACY IN THE DIGITAL AGE

In December 2013, the United Nations General Assembly adopted UN Resolution 68/167 on 'The Right to Privacy in the Digital Age'. This Resolution sought to strongly affirm the right to online privacy, noting that 'the rapid pace of technological development… enhances the capacity of governments, companies and individuals to undertake surveillance, interception and data collection which may violate human rights'. The Resolution came in the wake of the 2013 global surveillance disclosures by ex-National Security Agency (NSA) contractor Edward Snowden, who revealed the extent to which the NSA and its international partners conducted extensive unregulated surveillance of the telephone and online communications of foreign nationals and U.S. citizens. Political momentum for the Resolution was further ignited by Germany and Brazil; both countries pressed for the Resolution in light of reports that the heads of both states were victims of U.S. espionage in 2013.

Since then, continuous global efforts have been made to ensure that human rights law, particularly the right to privacy, keeps a pace with the rapid advancement in information and communications technologies in the Internet age.[24] However, given that the right to privacy is not absolute, there is an enduring tension between the protection of privacy rights and the national security interests of governments. The section below highlights some of the recent developments which have taken place in this area regarding governmental access demands which have sought to undermine the right to privacy.

Recent Developments: A Global Outlook

The UK's Data Retention Legislation, Apple vs FBI, and WhatsApp's end-to-end encryption

In 2006 the EU passed a Data Retention Directive which required each EU Member State to ensure that Communications Service Providers (CSPs) within their jurisdictions retain the communications data[25] of all their customers for at least six months and for no more than two years. The UK government complied with its obligations under this Directive by way of regulations passed in 2009. However, in April 2014, the Court of Justice of the European Union (the CJEU) in *Digital Rights Ireland* [26] struck down the EU Data Retention Directive on the basis that the mandatory and

[24] See "International Principles on the Application of Human Rights to Communications Surveillance" <https://en.necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf>; "Privacy Rights in the Digital Age: A Proposal for a New General Comment on the Right to Privacy under Article 17 of the ICCPR" <https://www.aclu.org/sites/default/files/assets/jus14-report-iccpr-web-rel1.pdf>; UN Doc A/HRC/28/L.27, appointing a Special Rapporteur on the right to privacy.

[25] The term 'communications data' encompasses metadata such as the identity of the sender and receiver of the communication, its duration, and the location from which it originated. It excludes the precise content of communications such as the text of emails or telephone conversations.

[26] *Digital Rights Ireland v Minister for Communications, Marine and Natural Resource* (Joined Cases C-293/12 and C-594/12) [2014] 3 WLR 1607.

indiscriminate retention of customer data amounted to a disproportionate interference with the right to privacy under articles 7 and 8 of the EU Charter of Fundamental Rights. The effect of this CJEU ruling was that the UK's 2009 Regulations now lacked a legal basis given that the EU's Directive was no longer operative. In response, the UK government hurriedly enacted the Data Retention and Investigatory Powers Act (DRIPA) in July 2014, which enabled the Secretary of State to issue retention notices to CSPs (such as Virgin, Sky, and BT) for the retention of communications data of every customer for up to 12 months.

In July 2015, in the decision of *Davis v Secretary of State for the Home Office*,[27] the Divisional Court declared DRIPA invalid on the basis that the legislation was inconsistent with EU law, in that it did not provide adequate safeguards for privacy rights as outlined by the CJEU in the *Digital Rights* case. In particular, it was held that the legislation lacked clear and precise rules for the access and use of retained data, and further, that access to the data was not made dependent on a prior review by a court or an independent administrative body.[28]

The decision in *Davis* was subsequently appealed and in November 2015, the England and Wales Court of Appeal ruled that it was unclear whether the CJEU intended to lay down mandatory requirements for all EU Member States in the *Digital Rights* decision.[29] The Court of Appeal therefore overturned the Divisional Court's ruling and referred the relevant questions to the CJEU regarding the effect of its *Digital Rights* judgment. The CJEU is yet to give its determination on the questions referred.

In the interim, the UK Home Secretary has introduced the Investigatory Powers Bill (the IPB) before Parliament as the successor to DRIPA, given that DRIPA has a sunset clause which terminates the Act in December 2016. A number of concerns have been raised about the extensive surveillance powers conferred by the IPB (nicknamed the 'Snoopers Charter' by its opponents), which requires Internet Service Providers to retain the browsing history of customers for 12 months, and to hand over such data to the authorities upon request.

In March 2016, a number of US tech companies[30] submitted a joint statement on the Bill before the UK Parliament.[31] In that statement, the companies rightly noted that the UK legislation has far-

[27] [2015] EWHC 2092 (Admin).

[28] Para 114.

[29] *Secretary of State for the Home Office v R (Davis and others)* [2015] EWCA Civ 1185.

[30] Apple Inc., Facebook Inc., Google Inc., Microsoft Corp, Twitter Inc. and Yahoo Inc.

[31] See: Investigatory Powers Bill: Written Evidence submitted by Apple Inc, Facebook Inc, Google Inc, Microsoft Corp, Twitter Inc. and Yahoo Inc. (IPB 21)
<http://www.publications.parliament.uk/pa/cm201516/cmpublic/investigatorypowers/Memo/IPB21.htm>

reaching implications and will likely set a precedent for similar legislation overseas. Further, the Bill purports to have extraterritorial jurisdiction in granting enforcement powers against UK employees of CSPs based outside the UK. The Bill also empowers security services to collect bulk communications data when deemed necessary for the protection of national security. The tech firms expressed concern about the necessity and proportionality of such bulk collection and the high level of intrusion associated therewith.

Another area of concern is that the Bill provides that tech companies may be served with a 'technical capability notice' which requires 'the removal of electronic protection where reasonably practicable'. U.S. tech companies have raised concerns over whether this provision may require them to create a back door for law enforcement which bypasses built in encryption mechanisms designed for the security of communication over their platforms. For example, in April 2016, WhatsApp introduced automatic end-to-end encryption for all messages and calls sent via that medium with the effect that no third party (not even WhatsApp itself) can intercept messages sent between a sender and recipient.[32] This means that, if requested, the company itself would not be able to give the content of communications to the government. This is significant when one considers that WhatsApp has over one billion users in various countries across the globe. The UK's IP Bill seems to contemplate the government having a residual power to require that such encryption be bypassed upon request from law enforcement. However, tech companies are strident that any such back door would greatly undermine the security of their platforms and would create vulnerabilities in their software which may be taken advantage of by cybercriminal actors.[33]

The battle over encryption also recently came to a head in the US in the case of *Apple Inc. v the Federal Bureau of Investigations (FBI)*. In February 2016, the tech company refused the FBI's order to assist it in unlocking an iPhone used by San Bernadino gunman Syed Farook. Apple maintained that designing software to undermine the security features of its phone would set a dangerous precedent. The United Nations High Commissioner for Human Rights issued a statement in support of Apple's position, noting that 'encryption and anonymity are needed as enablers of both freedom of expression and opinion, and the right to privacy'.[34] However, the case against Apple was discontinued in March 2016 after the US government's declaration that it successfully accessed the data stored on Farook's iPhone without Apple's assistance.

These events leave open the question of whether a law enforcement agency may lawfully compel a tech company to bypass its own security features. This question is yet to be judicially tested and

[32] See: David Meyer, "Here's why WhatsApp's Encryption is such a Big Deal" *Time* (California, 6 April 2016).

[33] Computer Science and Artificial Intelligence Laboratory Technical Report, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications (6 July 2015); Supra n 31.

[34] Office of the UN High Commissioner for Human Rights, "Apple-FBI case could have serious global ramifications for human rights" (4 March 2016) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138#sthash.o25R7Bqg.dpuf>

remains ripe for adjudication in both the U.S. and the UK in light of the developments mentioned above.

Continuing Challenges: Data Protection and Online Privacy in the Caribbean

So what bearing do these global developments have on the protection of privacy rights in the Caribbean? And, how robust are our own legislative frameworks in dealing with issues of data protection, cyber-security, and government surveillance?

First, it should be borne in mind that the recent developments concerning U.S. tech firms and UK legislation have global implications far beyond the borders of these two nations, and therefore necessarily concern the Caribbean region. Both countries are leaders in cyber-technology and their policies often shape international norms and opinions. It is therefore of great political significance if they are adopting policies which trend towards over-reaching state surveillance, a practice which they have previously decried in less open, authoritarian regimes. Further, given the expansive reach of these U.S. tech firms and the popularity of their platforms, any compromises in the level of security and encryption offered necessarily affect all their users worldwide. Additionally, online communication with those located within these countries (both of which possess very strong personal and business connections with the Caribbean) would be caught within the net of data contained on local servers in these states.

Secondly, it should not be assumed that Caribbean nations are safely insulated from surveillance conducted by the U.S. In 2014, Edward Snowden disclosed that the NSA was conducting extensive interception of telephone calls in the Bahamas, without the state's knowledge or consent, as part of a top-secret project, code-named SOMALGET.[35] This was reportedly done in order to uncover international narcotics traffickers. Given the unfortunate involvement of other Caribbean countries in the international drug trade, it is not unlikely that other nations in the region have been subject to such unauthorised surveillance.[36]

Caribbean states have also shown increased vulnerability to cyber-attacks and cybercrimes. Recent attacks include the theft of $150 million from the Bank of Nova Scotia (Jamaica) in 2014, the 2015 hacking of the government's website in St. Vincent and the Grenadines, and a ransomware attack on a number of Caribbean tax authorities.[37] In response to these threats, a number of Caribbean nations

[35] Ryan Devereaux, Glenn Greenwald and Laura Poitras "Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas" *The Intercept* (19 May 2014).

[36] See Michele Marius, "Spying in the Caribbean: some thoughts and considerations" *ICT Pulse* (28 May 2014).

[37] See: "Caribbean Nations Sign off on Cyber Crime Action Plan" (24 March 2016) http://www.telesurtv.net/english/news/Caribbean-Nations-Sign-off-on-Cyber-Crime-Action-Plan-20160324-0018.html

recently signed on to a regional plan of action to tackle cybercrime following a three-day workshop in St. Lucia in March 2016.[38]

There have also been attempts to assess and harmonize legislation in the region concerning data protection and the interception of communications. In 2012, the UN's International Telecommunication Union, in conjunction with CARICOM and others, conducted an extensive review of Information and Communication Technology (ICT) legislation in the region with a view to making recommendations for harmonization. This project was titled HIPCAR (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean). The HIPCAR report on data protection legislation reveals that most states do not possess an adequate statutory framework for the protection of personal data.[39] Figure 2, below, reveals these findings:

Country/Region	1. Legal Mandate	2. Institutional Framework	3. Regulatory Empowerment	4. Collection of Personal Information	5. Storage and Use of Information	6. Disclosure of Information
Antigua and Barbuda	NONE	NONE	NONE	NONE	NONE	NONE
Bahamas	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
Barbados	POOR	NONE	NONE	NONE	NONE	POOR
Belize	NONE	NONE	NONE	NONE	NONE	NONE
Dominica	NONE	NONE	NONE	NONE	NONE	NONE
Dominican Republic	NONE	NONE	NONE	NONE	NONE	NONE
Grenada	NONE	NONE	NONE	NONE	NONE	NONE
Guyana	NONE	NONE	NONE	NONE	NONE	NONE
Haiti	NONE	NONE	NONE	NONE	NONE	NONE
Jamaica	NONE	NONE	NONE	NONE	NONE	NONE
St. Kitts and Nevis	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
St. Lucia*	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
St. Vincent and the Grenadines	FAIR	POOR	FAIR	GOOD	FAIR	FAIR
Suriname	NONE	NONE	NONE	NONE	NONE	NONE
Trinidad and Tobago*	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED

Figure 2: Assessment of Data Protection Legislation in the Caribbean (Source: HIPCAR Report 2012)

[38] Commonwealth Cybercrime Initiative, Communique <http://thecommonwealth.org/sites/default/files/news-items/documents/6%20FinalCastriesDeclaration170316.pdf>

[39] International Telecommunication Union, "HIPCAR Privacy and Data Protection: Assessment Report" (2012) <http://www.itu.int/en/ITU-D/Projects/ITU-ECACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/privacy_and_data_protection_assessment.pdf>

A similar assessment was carried out regarding legislation relating to the interception of communications and whether these adequately addressed issues such as the basis for interception, confidentiality of intercepted communications, and safeguards against abuse.[40] The HIPCAR report summarised these findings in Figure 3, reproduced below:

Country/Region	Legal Mandate	Institutional Framework	Definition of Interception	Right to Intercept	Interception Approval	Confidentiality Measures	Monitoring	Interception Capabilities	Internal Safeguard Measures	Dispute Resolution
Antigua and Barbuda	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
The Bahamas	NONE	NONE	LIMITED	NONE	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Barbados	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Belize	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Dominica	LIMITED	LIMITED	LIMITED	FAIR	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Dominican Republic	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Grenada	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Guyana	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Haiti	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Jamaica	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
St. Kitts and Nevis	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Saint Lucia*	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD	GOOD
St. Vincent and the Grenadines	LIMITED	LIMITED	LIMITED	FAIR	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED	LIMITED
Suriname	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE
Trinidad and Tobago*	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE	NONE

Figure 3: Assessment of Interception of Communications Legislation in the Caribbean (Source: HIPCAR Report, 2012)

CONCLUSION

The rapid advancements in information technology continue to outpace the legal and regulatory frameworks within which these developments take place. Human rights law is by no means immune from the effect of these changes and must be adequately adapted in order to provide for a meaningful right to online and electronic privacy. While global initiatives continue to be made to modernise and advance this crucial right, it remains to be seen how effective these steps will be in curtailing some of the extensive surveillance powers which the U.S. and the UK now purport to exercise in the face of rising global terrorism. However, it is important to note that this debate cannot accurately be cast

[40] International Telecommunication Union, 'HIPCAR Interception of Communications: Assessment Report' (2012) <http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/interception_of_communication_assessment.pdf>

wholly as a trade-off between privacy and security in absolute terms, given that many of the purported encroachments to privacy, such as loosening encryption, may also operate to undermine cybersecurity in the short and long term.

Caribbean states, for the most part, do constitutionally safeguard the right to communications privacy and therefore possess the basic constitutional framework within which this right may be advanced. However, as noted in Figure 2, most states lack the implementing legislation necessary for the protection of this right, particularly as it relates to informational privacy through data protection laws. It is also worth noting that regional steps *are* being taken to fill these legislative gaps and to harmonize ICT policies and regulations across the region. It is hoped that these initiatives will soon bear meaningful fruit in the form of legislation which adequately balances the individual's right to privacy and the state's legitimate interests in its welfare and security.

Dr. Alecia Johns

April 8, 2016