The Bitter Cookie: Right to Cyber Privacy in Sri Lanka vs. the Misappropriation of Data Gathered Using Cookies

Gananath Gunawardena
Faculty of Law, General Sir John Kotelawala Defence University
nathgunawardena1388@gmail.com

Abstract— *Success and progress in the technological age is dependent on the ability to collect, process and disseminate information at lightning speeds, with incredible efficiency. Ironically, the same technology which improves life in the 21st century is often responsible for its setbacks. The use of cookies is a prime example of how convenience has come at a steep price. Through a qualitative analysis of legislation, case law, and academic opinion, this paper elaborates on how the use of cookies, if not properly regulated, can lead to violations of an individual's right to privacy, and how the Sri Lankan legal system is ill-equipped to discourage such violations. The study begins with the proposition that the right to cyber privacy exists as a positive legal right despite its absence from the Sri Lankan Constitution. It then elucidates the function of cookies as well as their constructive and destructive potential. The crux of the paper highlights the inadequacies within the Sri Lankan legal system, focusing on the Computer Crimes Act No. 24 of 2007 and the implications of what the author terms 'the "authorised" paradox'. Finally, it proposes certain amendments to the law with reference to international jurisprudence; specifically, the UK judgement in Vidal-Hall v. Google and the recent EU General Data Protection Regulation (GDPR).*

Keywords— **Cookies, Cyber Privacy, Computer Crimes Act No. 24 of 2007**

I. INTRODUCTION

As we entered the technological age, most aspects of our lives have been put 'online'. From everyday tasks such as researching for an assignment, shopping for groceries, paying utility bills, and interacting with friends and family, to more complicated activities like managing an entire business, getting a degree, or even seeking medical assistance, everything is being accomplished via computers, smartphones, and other devices linked together by the World Wide Web (Internet). Such advancements can be attributed to our significantly enhanced ability to collect, process and disseminate information at lightning speeds with incredible efficiency. Ironically, these same capabilities which allow anyone with a computer to perform these activities with just a few clicks can also enable another person with a computer to interfere with such activity. Therefore, increased convenience in this modern age has come at a steep price- ranging from the risk of personal embarrassment to severe financial loss. This has given rise to a multitude of legal issues, where the violation of an individual's privacy stands out as a major concern. The use of cookies is a prime example of how advancements in Information Communication Technology can act as a double-edged sword.

This paper focuses on how the use of cookies, if not properly regulated, can lead to violations of an individual's right to privacy and what solutions exist to mitigate such violations. The arguments presented in this paper are based on the premise that the right to privacy exists as an actual legal right. Therefore, the first part of this paper discusses (quite briefly) how such a right does exist within the Sri Lankan legal framework, despite it not being given express recognition as a Fundamental Right. The second part of the paper explains what Cookies are, their basic function, and the positive aspects of their use. Next, attention will be focused on the different ways in which cookies pose a threat to individual privacy. (Here, special emphasis shall be placed on the fact that most data collected using cookies is, technically, 'authorized' by the user and hence, cannot be classified as unauthorized access. This paper argues that this can still amount to a violation of privacy, on several different levels, notwithstanding such data being obtained with consent.) The final part of this paper determines that Sri Lanka's existing legal regime is inadequate to prevent or punish such violations of privacy, and attempts to remedy it by advocating for certain alternative solutions proposed internationally.

III. THE RIGHT TO PRIVACY HIDDEN WITHIN CHAPTER III

The extent to which the right to privacy exists within the Sri Lankan legal regime warrants separate research and analysis in itself, owing to the fact that it has not been expressly recognised under Chapter III. Moreover, the specific right to privacy in cyberspace has not been given express recognition by the Electronic Transactions Act No. 19 of 2006, nor the Computer Crimes Act No. 24 of 2007- the two main pieces of legislation within the sphere of Sri Lankan IT Law. Such a thorough analysis cannot be entertained within the confines of this paper, without distracting too much from its principle topic.

The most convincing argument supporting the existence of the right to privacy as a Fundamental Right is that the freedom of speech and expression including publication guaranteed by Article 14 (1) (a) of the

Constitution can be interpreted to also include the right NOT (emphasis added) to express, or to consider silence as a form of expression in itself. This would mean that a person communicating with a specific individual/ individuals has the right to have that communication kept private from any third party. This argument has been propounded at length by Althaf Masoof (Masoof 2007).

In the context of cyber privacy, it can be argued that provisions prohibiting unauthorized access (Computer Crimes Act 2007, s. 3), obtaining information without lawful authority (Computer Crimes Act 2007, s. 7), and illegal interception of data (Computer Crimes Act 2007, s. 8), implicitly recognise a right to cyber privacy within Sri Lanka.

Moreover, the right to privacy in cyberspace has been given express recognition under international law by instruments such as the UN Guidelines for Regulation of Computerized Personal Data Files of 1989 and the UN General Assembly Resolution on Right to Privacy in the Digital Age 2013. In the UK, the Data Protection Act of 1998 grants similar express recognition. In light of all this, it is quite safe to argue that the right to privacy in cyberspace can and should be respected as a legal right.

IV. WHO WANTS A COOKIE?

A cookie is a small piece of information written to the hard drive of an Internet user when he or she visits a website that offers cookies. Cookies can contain a variety of information, including the name of the website that issued them, where on the site the user visited, passwords, and even user names and credit card numbers that have been supplied via forms (Eichelberger 2017). Cookies can either be temporary- where they only last until the end of a single web session, or persistent- lasting across several browsing sessions until they are cleared by the user.

A detailed analysis of how data is gathered using cookies can be found in *Re Double Click (S.D.N.Y. 2001) 154 F.Supp.2d 497*; a class action law suit filed before a US Federal Court where the plaintiff class claimed that DoubleClick's cookie policy was in violation of several US federal laws pertaining to data protection. The legal implications of this case will be addressed towards the latter part of this essay while, for the time being, this would serve as adequate reference regarding the technological intricacies of cookie-use from a legal point of view.

In the context of this analysis, it is noteworthy to mention that all cookies are more or less stored on a user's hard drive with his consent. Some newer web browsers come with cookies turned off by default and all browsers provide the option of clearing cookies or blocking them to varying extents. Most websites will also ask a user whether he wishes to accept or reject cookies. The latter part of this essay discusses how this can still amount to a violation of a user's right to cyber privacy.

V. COOKIES ARE SUPPOSED TO BE SWEET

Despite the 'darker' side of this particular breed of technology which this essay focuses on; i.e. the threats it may pose to user privacy, it is important to note that cookies are predominantly beneficial, and have made internet browsing a lot more convenient.

Cookies are immensely helpful to repeat visitors on a particular website. The information it has stored from a previous visit will allow the user to avoid data traffic and thereby load the web page faster, or if the site requires you to login, such login information can also be stored on the cookie making the entire process much more convenient. Once inside the website, the cookie may store certain user preferences such as auto-fill data (details previously entered into a form on the site such as name, address, telephone numbers etc.), search keywords, frequently visited parts of the site, and advertisements viewed. All this information is used by the website to provide the user with a browsing experience customised to his needs and preferences, with an increased level of convenience. For example, one may notice that an online shopping website such as eBay displays advertisements of products similar to the ones viewed on a previous visit. Many people find such customisation to be extremely useful in getting the best deals for whatever products they are looking for.

At the same time, the use of cookies can be immensely beneficial to the creators of a website as well. In addition to the abovementioned information, a cookie may also record how long a user remains on the site or which areas of a webpage he frequently clicks on. Such information is analysed by certain websites in order to obtain valuable feedback regarding how popular the site is, how users locate the site, and which areas of the page are best suited to display advertisements. This information is then used by the site-owners to expand their reach, and to improve on-page advertising.

Therefore, the use of Cookies is, for the most part, beneficial to both parties involved and its proper use will make web browsing more convenient for the browser, while allowing the web designers to improve their sites.

VI. WHEN THE COOKIE TURNS BITTER

As exhorted above, cookies are predominantly beneficial and are offered subject to the consent of the user. How then, does this simple piece of technology violate a person's right to cyber privacy?

'Third party cookies' and 'tracking or tracing cookies' pose the greatest risk to user privacy. A third party cookie is one which is not offered by the same website a user is currently viewing:

> '…users quite often find in their computer files, cookies from web sites that they have never visited. These cookies are usually set by companies that sell internet advertising on behalf of other web sites. Therefore it may be possible that users' information is passed to third party web sites without the users' knowledge or consent, such as information on surfing habits. This is the most common reason for people rejecting or fearing cookies'. (Cookies: Frequently asked questions 2017)

A tracking cookie enables the creation of a user profile containing a web user's preferences and browsing habits:

> 'Tracking or tracing cookies are the most threatening to a user's privacy as they may be used to compile a profile of a user's Web surfing habits across multiple Web sites. Whereas a regular cookie enables a Web site operator to develop a profile about a user based upon his or her actions solely on a that operator's site, tracking or tracing cookies go a step further by tracking and reporting information about actions taken on several different Web sites. This enables the Web site operator to compile a much deeper profile of the user's behavior and interests.' (Cookies- Overview 2007)

An assessment of the capabilities of these two types of cookies illustrate the threat of user information being collected by third-party websites, which in turn can be used to create user profiles containing a detailed account of browsing habits across several hundred websites. This is akin to a person borrowing books from several different libraries over the course of many years, while all that information regarding the books he borrowed and how long he spent reading each book is recorded on a single library card.

The main purpose for which such profiles are used is to produce 'targeted ads' which is often utilised by companies providing Online Behavioural Advertising (OBA) services to match the advertisements you see while browsing, with your interests (Privacy Fact Sheet 4: Online Behavioural Advertising; Know Your Options) While this alone can be understood to be a palpable threat to user privacy in and of itself, the possibility of this information being sold for monetary gain is an even graver concern in today's commercially driven world.

There exist even greater threats to user privacy when such information is made available to non-advertising entities. Dyrli argues that users who look up information on topics such as abortion, capital punishment or gun control, stand a chance of being subjected to harassment by special interest groups (Dyrli 1997). David Christle presents the hypothetical where a person who frequents sites promoting alcohol, has that information being made available to his insurance company, which in turn increases his premium (Christle 1996). White refers to arrests made by the FBI based on a person's activity on Pornographic websites (White 1995). If data collected using cookies is made available to law enforcement, it is not ludicrous assume that it may lead to arrests being made on such grounds. Although some might argue that these are extreme examples, given the current politico-economic climate, one cannot declare that such fears are completely unfounded. In the technological age where information is freely available and easily traceable, it is important to acknowledge that cookie technology has opened the door to such potential violations of cyber privacy and that it is only a matter of time before man starts stampeding through it.

VII. THE 'AUTHORISED' PARADOX

As stated previously, cookies are often offered with the consent of the user in some form or the other. This section questions whether there is 'true consent' in all such instances. Before browsers such as Microsoft Explorer and Netscape came with cookies disabled by default, users had to change their settings in order to block all or specific types of cookies (Privacy Fact Sheet 4: Online Behavioural Advertising; Know Your Options). This remains true with regard to most popular browsers today. In such a case, can a web user (a vast majority) who isn't aware of what cookies do or how to disable them, be regarded as an individual who truly consented?

Most browsers that do not have cookies disabled by default, do contain that fact, buried deep within their terms and conditions, which is hardly ever read in practice. Moreover, some websites offer cookies by default, making it the user's duty to disable it on his browser. However, in recent times, most websites display a notice requesting permission to offer cookies on their page. Despite such safeguards to ensure active user consent, there are still two major issues that may arise: Firstly, in a crowded website with many banner advertisements, it may be difficult for a user to distinguish between cookies offered by the main site and those offered by external ones (first party cookies v. third party cookies). In such an instance, does a user who consents to receiving cookies on a particular site also consent to receiving third party cookies? As pointed out earlier, it is these third party cookies that pose the greater threat to user privacy. Secondly, some sites cannot be accessed at all unless the user enables cookies. In such a context, it is debatable as to whether this amounts to 'true consent'.

VIII. MAKING THE BITTER COOKIE, BETTER

At this juncture, it is pertinent to examine existing domestic legislation regarding the legal threshold necessary for criminalising acts of the nature contemplated in this essay. In Sri Lanka, the law is

predominantly found within the provisions of the Computer Crimes Act No. 24 of 2007 which lists out 8 different computer-related offences. The offence defined under Section 5; causing a computer to perform a function without lawful authority (commonly known as cracking) is irrelevant to this discussion since a cookie will merely collect data rather than perform a function. The Section 6 offence is one committed against national security, economy or public order and is therefore excluded. Section 8 makes it an offence to unlawfully intercept data and is also irrelevant to the discussion since cookies perform no interception. Section 9 relates to the use of illegal devices. Although a cookie can arguably fall within the definition of a 'device' under this provision, it will be impossible to establish '…intent that it be used by any person for the purpose of committing an offence under this Act' as will be evidenced through the subsequent analysis. Therefore, only the offences defined under Sections 3, 4, 7, and 10 are of even remote relevance to this discussion, warranting closer examination and analysis.

Sections 3 and 4 both require the element of 'unauthorised access' and constitute the offence commonly known as 'hacking'. Since the statute does not define 'access', it is difficult to make a convincing argument that placing a cookie on a user's hard drive would constitute access. Notwithstanding this difficulty, it is a near impossibility to argue that the placing of a cookie was 'unauthorised', since this term is also not defined by the statute and, as discussed previously, there is always some level of consent rendering it 'authorised' within the ordinary grammatical meaning.

Section 7 would be the most appropriate provision for the purpose of criminalising the misuse of cookies since it deals with the obtaining of data which is the express function of a cookie. However, the provision, as it stands, will be of no assistance since it also requires that the data be obtained 'unlawfully'. Hence, it will require the introduction of an interpretative clause, narrowly defining 'unauthorised' to mean 'without express consent', in order for this provision to be effective in criminalising the threats described above. However, the author believes that this will prove to be relatively ineffective and may lead to unnecessary complication of the law. Therefore, a more pragmatic solution is proposed in the following paragraph.

Section 10 which deals with 'unauthorised disclosure of information enabling access to a service' does not afford a direct solution since cookie data does not 'enable access'. However, a closer look at the language of Section 10 reveals the possibility of creating an offence, even when data has been lawfully obtained:

'Any person who, being ENTRUSTED WITH INFORMATION (emphasis mine) provided by means of a computer, discloses such information without any express authority to do so or in breach of any contract expressed or implied, shall be guilty of an offence.'

The author therefore advocates for the introduction of a new offence, combining Sections 7 and 10, prohibiting the 'misappropriation of lawfully gathered data'. Here, 'misappropriation' would include 'buying, selling, receiving, retaining or in any manner dealing with such data, for a purpose that was not expressly authorised at the time at which such data was obtained.'

IX. THE COOKIE PUT ON TRIAL

Attempts to penalise privacy violations caused by the use of cookies has encountered the same obstacle in other jurisdictions. In *Re Double Click* (S.D.N.Y. 2001) 154 F.Supp.2d 497, which was referred to previously, the plaintiff class based their claim on alleged breaches of the Electronic Communications Privacy Act (ECPA), the Federal Wiretap Act, and the Computer Fraud and Abuse Act (CFAA). The action was dismissed on the grounds that the impugned acts fell within the consent exceptions of the first two statutes and did not reach the required 5000$ threshold of statutory losses under the third statute. Two other class action suits based on the same three statutes were dismissed on similar grounds; *Re Intuit Privacy Litigation* (C.D. Cal 2001) 138 F. Supp. 2d 1272 which dealt with first party cookies, and *Chance v. Avenue A, Inc.* (W.D. Wash. 2001) 165 F. Supp. 2d 1153 where the use of cookies to create targeted advertisements was challenged. A more severe blow was dealt to privacy advocates in *Re Pharmatrak, Inc. Privacy Litigation* 292 F. Supp. 2d 263, where the plaintiff class instigated action against a pharmaceutical company which had created detailed profiles of clients' medical conditions, occupations and insurance information in the manner previously discussed in this essay. The plaintiff class moved the court to narrow the scope of permission given to Pharmatrak, so they could only collect 'anonymous, aggregate information' as opposed to 'personal, detailed information' but their motion was denied.

Despite such failure to successfully maintain an action in the USA, on the other side of the Atlantic, a recent case has broken new ground in the field of cyber privacy; *Vidal-Hall and others v Google Inc.* (2014) EWCA Civ 311. The claimants' action was based on the distress suffered from learning that their personal browsing habits collected by Google using cookies on the Safari browser were used to create targeted advertisements. The claimants relied on the torts of misuse of private information and breach of confidence as well as provisions of the Data Protection Act of 1998. The High Court judgment, delivered in favour of the claimants, was subsequently upheld by the Court of Appeals. This judgement has laid down two important principles of law which will facilitate similar claims in the future: Firstly, it has cemented the misuse of private information as a tort

that would also apply to provisions of the Data Protection Act. Secondly, it allowed claims based on non-pecuniary loss which proved a major obstacle under the previously discussed US legal regime. Both of these principles could prove useful in the Sri Lankan context as grounds for pursuing litigation on common law bases, even in the absence of legislation. Although the Sri Lankan law of Delict is based on Roman Dutch Law, it has been heavily influenced by principles of English Tort Law. For example, the principle of strict liability, borrowed from the seminal English case of *Rylands v. Fletcher* (1868) LR 3 HL 330, is completely foreign to Roman Dutch Law, but was applied by a full bench of the Sri Lankan Supreme Court in *Elphinstone v. Bouste (*Ram (1872-76) 269) which was later upheld in *Silva v. Silva* (1914) 17 NLR 2. However, the author presents judicial activism as a last resort, which is not likely to succeed on its own, since later judicial trends have shown a reluctance on the part of the courts to extend the judicial incorporation of English law (Cooray 1972). The author maintains that it is more pertinent to utilise the common law in order to persuade a change in legislation and subsequently support legislation that introduce these principles.

X. THE COOKIE ABROAD

The European Union (EU) has made great strides in terms of regulating the use of cookies through legislation passed by the European Parliament and the Council of the European Union. Therefore, a cursory examination of these laws would provide a better understanding of how to legislate on this matter.

Under EU law, websites must comply with the commission's guidelines on privacy and data protection provided under *Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications*. Article 5 (3) of the Directive specifically requires websites to obtain informed consent from web uses by providing 'clear and comprehensive information in accordance with Directive 95/46/EC'. This Directive was recently repealed and replaced by the more stringent *Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,* commonly known as the General Data Protection Regulation (GDPR). This infamous regulation which came into force on the 25th of May 2018, caused a complete overhaul of the terms and conditions on most websites. The regulation identifies cookies under Clause 30 where it provides that if a cookie can identify a user it is considered personal data and therefore subject to the provisions of the Regulation.

These Regulations and Directives can be used to identify the points of concern with regard to the use of cookies, pinpoint the aspects of cookie-use which can be regulated by the law, and ultimately understand ways in which they can be effectively regulated. This would prove invaluable in the formulation of domestic laws for regulating the use of cookies.

XI. CONCLUSION

Over the past few decades, the humble cookie has developed into an integral part of the web browsing experience- making it faster and more convenient for the users, while helping designers improve their sites. However, the same technology that makes cookies such efficient collectors and trackers of information is what makes them equally exploitable and dangerous as instruments of privacy violations. An individual's right to privacy is an internationally recognised Human Right and the author argues that this right is also recognised implicitly under the Sri Lankan Constitution. However, this essay highlights the fact that Sri Lankan cyber law, as it stands today, is not even remotely equiped to address the threats posed by the abuse of cookies or similar technology. This is mainly due to the fact that, under Sri Lankan law, data obtained with consent falls under the exception of being 'authorised' conduct and is thus excluded from liability. Notwithstanding, this essay also recognises several instances where even lawfully obtained data can be later misused. Internationally, these threats to user privacy have been realised, and attempts have been made to pursue litigation in that regard. Despite its slow progress and despite the initial reluctance of courts to penalise such infractions, there has been significant development in this area, especially since the Vidal-Hall judgment. The author advocates for similar development domestically, preferably through the proposed legislative amendments to the Computer Crimes Act or, failing which, through judicial activism borrowing from international jurisprudence. This would render even the bitter cookie, a lot more palatable.

REFERENCES

Computer Crimes Act No. 24 of 2007

Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications

Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

Chance v. Avenue A, Inc. (W.D. Wash. 2001) 165 F. Supp. 2d 1153

Re Double Click (S.D.N.Y. 2001) 154 F.Supp.2d 497

Re Intuit Privacy Litigation (C.D. Cal 2001) 138 F. Supp. 2d

Re Pharmatrak, Inc. Privacy Legislation (D. Mass 2002) 292 F. Supp. 2d 263

Vidal-Hall and others v Google Inc. EWCA Civ 311

Christle D, (1996) *The Controversial Cookies.Txt!.* Available from: http://www.cookiecentral.com/ccstory/cc3.htm. (accessed 20 September 2017).

Cooray, LJM, (1972) *An Introduction to the Legal System of Sri Lanka*, (1st Pub) Stamford Lake Publication

White M, (1995) *Don't Count on Confidential E-Mail*. Available from: http://www.cookiecentral.com/ccstory/cc3.htm. (accessed 20 September 2017)

Masoof A, (2007) Privacy Related Computer Crimes; A Critical Review of the Computer Crimes Act of Sri Lanka, Sri Lanka LCL Rev 5

Masoof A, (2008) *The Right to Privacy in the Information Era: A South Asian Perspective*. Available from: https://script-ed.org/wp-content/uploads/2016/07/5-3-Marsoof.pdf. (accessed 21 August 2017)

Dyrli O, (1997) Online Privacy and the Cookies Controversy, Technology & Learning 20

Eichelberger L, *The Cookie Controversy.* Available from: http://www.cookiecentral.com/ccstory/cc3.htm. (accessed 19 August 2017)

About Cookies, *Cookies: Frequently Asked Questions.* Available from: https://www.aboutcookies.org/cookie-faq/. (accessed 28 August 2017)

Cookies and Online Privacy, *Cookies- Overview.* Available from: https://www.unc.edu/courses/2006spring/law/357c/001/projects/jhubbard/cookies2.html. (accessed 28 August 2017)

Office of the Australian Information Commissioner, *Privacy Fact Sheet 4: Online Behavioural Advertising; Know Your Options.* Available from: https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-4-online-behavioural-advertising-know-your-options. (accessed 18 September 2017)

The EU Internet Handbook, *Data Protection.* Available from: http://ec.europa.eu/ipg/basics/legal/data_protection/index_en.htm (accessed 21 July 2018)