Paper ID: 501

Challenges in investigating Cybercrime in social networks: A Sri Lankan Perspective

K. G. Laksiri Geethal[1], Kasun De Zoysa[2], Kenneth Thilakarathna[3#,] Primal Wijesekera[4] and Chamath Keppitiyagama[5]

[1]Sri Lanka Police

[2,3,5]University of Colombo School of Computing

[4] University of California, Berkeley + ICSI, USA

[#]kmt@ucsc.cmb.ac.lk

Abstract: With the explosive growth of social networks, the modern society has found itself in the midst of a transformation from pre-social network age to a new world where social networks influence everything from democratic processes such as elections to the mental health of the members of the society. While arguing the net cost and benefits of social networks are out of the scope of this case study, we will argue that social networks have introduced a new threat surface that challenges the current status quo on legal protection and investigative techniques on citizens. These challenges equally affect citizens who request justice and protection, and people who are hiding and avoiding law enforcement.

From the perspective of a developing nation, especially a nation that does not host any technical infrastructure for any leading social network companies, this work presents challenges Sri Lanka could face and discuss their impact on law enforcement investigations. We believe this case study will open up discussions on the proper legal framework to support future investigations.

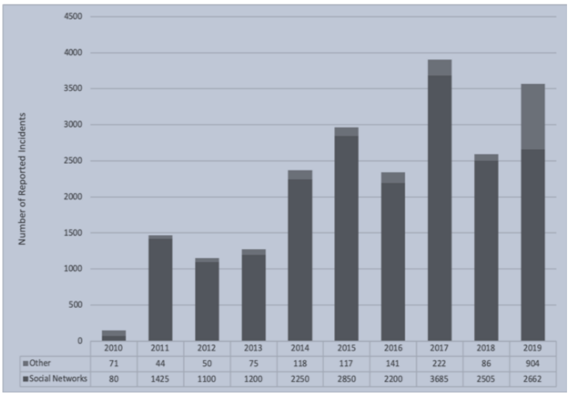
Keywords: Social Networks, Social Media, Law Enforcement, User Privacy, Privacy Expectations, International Jurisdiction.

Introduction

The evolution of information communication technology and social network applications have made the world smaller and more connected than it used to be. Over the last decade, social networks took the helm as the most prevalent software in society. We define a social network as any service that offers a community like interaction to users such as Facebook, LinkedIn, TikTok, WhatsApp (Jan H.Kietzmann, et al., 2011). These social networks provide a host of societal benefits that promote freedom of speech, a sense of connectivity, and a place to help each other (Shirky, 2011). Social networks, however, were found to be a source for increased mental health (Rachel L.Frost & Debra J.Rickwood, 2017), cyberbullying (Grace Chi En Kwan & Marko M. Skoric, 2013), a place for vast cyber black market (Paullet, Karen & Pinchot, Jamie, 2012), and sextortion (Mirjana Gavrilovic Nilsson, et al., 2019) – This list is not exhaustive. Among those listed issues, the biggest of all is finding and bringing those responsible for these crimes. Social networks are, by nature, complexed social-techno systems (Jessa Lingel & Adam Golub, 2015), and one downside of that complexity is, it is easy to hide the real identity of people involved in these crimes behind digital avatar (Joshua Brunty & Katherine Helenek, 2012). Such an ability to hide provides users with a criminal instinct to make use of social networks to carry out their unlawful activities (Karabiyik, et al., 2016) (Nova, et al., 2018) (Desmond Upton Patton, et al., 2014).

Sri Lankan Statistics

According to the Criminal Investigation Department (CID) statistics and Sri Lanka Computer Emergency Readiness Team | Co-ordination Center (SLCERT|CC), cybercrime activities increase every year. According to the Annual Activity Report – 2019, the percentage of incidents reported to Sri Lanka CERT connected to a social network is consistently high over the last decade (SLCERT|CC, 2019). illustrates the growth of Cybersecurity incidents in social networks comparing with all other incidents reported to SLCERT|CC.



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
■ Other	71	44	50	75	118	117	141	222	86	904
■ Social Networks	80	1425	1100	1200	2250	2850	2200	3685	2505	2662

Figure 39: Growth of Cyber-security Incidents reported to SLCERT|CC

contains an extract of the statistics on the number of Cybercrime activities reported to the CID of Sri Lanka with a breakdown of the medium of the crime. Though digital crimes span across several approaches, our focus is on victimization carried out using social network users/ accounts. We analysed censored reports on investigations of selected cases to gather information. Among the incidents analysed, there were cases concerning bullying in cyberspace, cyberstalking, defamation, pornography, Nigerian or "419" Fraud Scheme (Investigation, n.d.), and impersonation.

In the first quarter of 2020, over 87% of 13 million Internet users in Sri Lanka estimated to be using Mobile Broadband connections (TRCSL, 2020). There are around 11 million Internet users having Internet access from almost anywhere.

Table 1: Reported Computer Crimes to CID of Sri Lanka

	Categories of Cybercrime			
Year	Social Networks	Unauthorized Access	Emails	Total
2009	34	2	8	44
2010	61	6	15	82
2011	115	12	34	161
2012	62	11	31	104
2013	23	6	16	45
2014	80	12	22	114
2015	175	15	3 0	220
2016	170	17	35	222

Reports indicate that there are over 6 million social network users in Sri Lanka as of January 2020, and the number of users increases by year (KEMP, 2020). However, increased use of the social network has also proportionately increased the number of crimes committed.

At this stage of the research we were unable to get the exact number or resolved cases. However, according to discussions with the relevant offices, much of the cases reported to CID were not investigated or resulted in a conviction. Lack of legislative support for social network Cybercrime and Internet Service Providers (ISP) do not keep sufficient amount of details about user activities to derive required evidence were highlighted during the interviews.

Legal Background

A crime initiated over the social network needs to accompany a digital device with computational power such as a mobile phone, laptop computer, or tablet computer. The device may have been used in many ways to commit the crime. Instead of reaching the victim in person, the victim's computer or mobile device would be an alternative target. An attack may be initiated by merely making the victim open a spreadsheet application where even an anti-virus program would not identify the file to be evil. Legislation and legal provisioning have already been established in Sri Lanka in provisioning the required legislative protection for citizens victimizing from such crimes through "Computer Crime Act, No. 24 of 2007" (PARLIAMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA, 2007). It defines and describes what is considered an offense, how compensation is awarded for loss or damage due to an offense, provisions concerning the investigations, and procedures for a "Computer crime." Further, in the recent past, there have been initiatives to accede with the Budapest Cybercrime Convention of the Council of Europe in resolving limitations such as multi-jurisdictional investigations (Europe, 2001). It was also identified that there are multiple Acts related to the Computer Crime Act, No. 24 of 2007, such as Code of Criminal Procedure Act, No. 15 of 1979, Extradition Law, No. 8 of 1977, Payment Devices Frauds Act, No. 30 of 2006, Obscene Publication Act. No. 22 of 1983, Penal Code No. 02 of 1883, Electronic Transactions Act No. 19 of 2006, Information and Communication Technology Act No. 27 of 2003, Intellectual Property Act No. 36 of 2003, and Payment and Settlement Systems Act No. 28 of 2005.

Investigative Challenges

Here we list different categories of challenges criminal investigators could face.

A. Multiple Jurisdiction Challenges

According to CID, gathering valid evidence against accused from social networks is challenging. There is literature discussing the possibility of extracting evidence from social networks (Kathryn C. Seigfried-Spellar & Sean C. Leshney, 2016). However, with the controls in place to protect social network user accounts, the amount of data that can be extracted is limited (SON, 2012). Following data misuse scandals reported recently, many social network service providers further restricted access to the information making the data extraction much more limited (Archibong, 2018). While it is hard to speculate, tighter restrictions are imposed for user protection or as a marketing tactic to count fear of government surveillance (Scott, 2017). In the recent past, tech companies like Apple, Google, Microsoft, and Facebook have used denying government requests for data as a media circus to portray themselves as guardians of user data (Feiner, 2020). Answering the question of who is being more responsible for the greater good of the society remains tricky; in the meantime, this will present a more significant threat to a proper investigation of many important legal cases. As a result, it will hinder prosecuting criminals.

Unsupportive social networks are a global threat to law enforcement. However, countries like Sri Lanka have a more severe challenge in pursuing criminal investigations – under whose jurisdiction these big tech companies fall. In the infamous case of unveiling the "Silk Road" underworld marketplace (Bearman & Hanuka, 2015), the reporting of the case highlighted multi-jurisdiction issues. With tech companies situated in other countries under different laws and regulations, countries such as Sri Lanka faces the daunting task of getting their requests processed by those companies. Given the social-economic status of Sri Lanka, the question is, what incentivizes these tech companies to comply with the Government of Sri Lanka? So far, we have seen Facebook keenly helping Sri Lanka it tackling the spread of fake news, although Facebook was not complying initially (Reporter UCA News, 2020). However, no public records are available on government requests to Facebook concerning criminal investigations.

B. Legal Challenges

Another aspect that comes with multi-jurisdiction is how global laws on data protection and privacy affect criminal investigation in countries like Sri Lanka. Most of these big tech companies have data servers span across the world, and most of the latest wave privacy regulations, such as General Data Protection Regulation (GDPR), have relied on the location of the data server in question (Catherine Jasserand, 2018). However, it still an open question of how the said purpose of data collection will come into play when companies are to comply with government requests. For example, can a third-party service such as Facebook, who collect logged IPs, and locations for advertising purposes, share such information for a criminal investigation? Because the later is different from the original data collection purpose. GDPR is forcing everyone to be upfront about their data collection, and respective purposes and such purposes never include sharing their user data with governments. Such an acknowledgment will negatively impact the tech firm’s trust. Given that GDPR is the first global-scale privacy regulation, most global tech companies are adopting to avoid fines. We envision GDPR will come into play in many Sri Lankan investigations as well.

Another aspect of GDPR that is likely to affect criminal investigations in Sri Lanka is the “*right to be forgotten*” directive in GDPR (Zaman & Hassani, 2019). Under GDPR, users can ask tech companies to delete any data related to the given user. Such requests could potentially delete important evidence related to a criminal investigation. While the probability of that happening is still theoretical, it is crucial to be aware of these situations that could roadblock an investigation.

C. Technical Challenges

In a social network, each user has a perceived identity (or avatars). Criminals or even average citizens do not have real information on social networks (Krombholz, Katharina, et al., 2012). Criminals do that to avoid legal action, and others do that for privacy reasons. Identifying real people behind social network avatars (de-anonymizing) is why people are still looking for a solution (Narayanan & Shmatikov, 2009). Identifying the relationship between two avatars from different social networks does not reveal a person's real identity who may be involved in the act of crime. Another technical challenge along anonymization is the dark web and related technologies (Jardine, 2015) (David Goldschlag, et al., 1999). By nature, these techniques are designed to hide identities and other information that could pinpoint a real person. Investigating "silk road," such technologies are shown to be a significant technical challenge even to nations such as the US, Canada, Europe with vast technical tools at disposal (Joshuah Bearman & Tomer Hanuka, 2015). Such techniques have the capability of completely derailing an ongoing investigation. We believe that outside of legal challenges, the dark web and related technologies pose the biggest threat.

D. Privacy Challenges

Privacy and data protection play a prominent role in mitigating risks and achieving trust for any organization, even for a government. However, according to the United Nations Conference on Trade and Development (UNCTAD) 2019, Sri Lanka does not have any legislation on Privacy and Data Protection (Senaratne, 2020) (UNCTD, n.d.).

Especially the children in this modern society dealing in cyberspace create a dangerous situation for themselves. In Sri Lanka, a schoolgirl committed suicide because of a relationship she developed within the cyberspace. She took her life because she could not bear the mental agony she underwent. According to the incidents reported to the Child Protection Authority, there are incidents where school girls became mothers. Consequently, some went abroad because they could not face the society. This situation has created a great danger within Sri Lankan society. Children's Online Privacy Protection Rule (COPPA) in the US is one of the most stringent privacy laws safeguarding children online (Szoka, Berin & Thierer, Adam, 2009), and GDPR also has provisions for kids. We present children’s privacy as a use case where a lack of regulations might block investigators from the necessary tools to go after criminals. Nowadays, criminals use every possible tool they possess to exploit victims, and so should law enforcement possess every tool they can use.

E. Open Source Intelligence

One of the biggest advantage on social network is the elevated role of open source intelligence (OSI). Open source intelligence focuses on gathering evidence based on publicly available data mainly data available in social networks. Organizations such as Bellingcat performs crucial investigations for both public safety and for legal cases crowdsourcing evidence collection based on data available online. The effectiveness of OSI in a criminal investigation relies heavily on the nature of investigation.

While OSI will not be a tool for every social network investigation, it is important to understand availability of tools such as OSI for evidence collection. This is even more important as a low cost solution for countries like Sri Lanka. If the data is publicly available, accessing such data for an investigation will not violate user privacy.

Discussion

Convicting a person requires an entity that can be produced to the court of law. The study was carried out to identify the challenges of mapping a virtual person to a real person produced to the court of law. This mapping requires the information from multiple sources such as social network service providers, ISPs, telecommunication service providers, etc.. For this study, the most vital information to map a virtual person to a real person lies with the social network service provider. However, every case we studied, the social network service provider is from outside the country and governed by different jurisdictions. Additionally, they are abiding by the privacy policies and laws that are in place to build trust and minimize their users' risk. Therefore, retrieving such information is an enormous process. This may be one of the reasons for investigations of some cases that have to be put on hold for years. The privacy laws intended to protect people have provided hiding grounds to malicious users at least by making the investigation more difficult or sometimes practically infeasible due to transnational jurisdictions.

Even after obtaining the information from the social network service provider, the information should be correlated with other supporting digital evidence from the rest of the information sources. One of the main limitations that has been encountered in investigations was information sources such as ISPs do not keep the user activity information with sufficient amount of details. Further, lack of policies on information classification lead to shorter retention period for information that are important for Cybercrime investigations.

In a situation where Internet communication anonymizers (Jardine, 2015) (David Goldschlag, et al., 1999) have been used by the suspect, the investigation process becomes more challenging. Much research has been carried out on de-anonymize social networks using different approaches. Most of the research has not focused on de-anonymization targeted for a particular avatar, which is the practical need in conducting those above digital forensic investigations.

Employing social engineering methods on suspects to identify their identity has been successful for a considerable amount of cases. Improved skills and tools would have served better for their endeavors. Conducting an investigation is quite different from hacking into a system—this further narrow down techniques and approaches that can be employed for digital forensic investigations.

Although our work focuses on proceeding criminal investigations on social networks, the other side of this topic is user privacy. Users are globally wary of the reach of the government into their personal life, and with a fully connected digital infrastructure, their concerns have become a reality. While there is no black-&-white answer to this concern, the most acceptable answer is to create a dialog and let different stakeholders voice their concerns.

In the Sri Lankan context, consumers lack a proper legal framework to protect themselves against unlawful government reach; however, even for a legitimate criminal investigation, law enforcement might lack tools. The future of this dialog should focus on low-cost techniques that suit countries like Sri Lanka. In the meantime, proper steps should be taken to protect consumer privacy. Such laws are not meant not to impede any legal consumer protections but to increase consumer confidence, protect consumers from other malicious users roaming in social networks.

Criminal investigations on social networks are still young in many ways. However, given the statistics shown above, the crime rate involving social networks have gained space and as a nation and for the sake of law enforcement, proper tools and legal protection should be available for the betterment of the society.

Evidence Based Strategy

Regardless of the paper's challenges, as a nation, we need astrategy on how to cope up with cybersecurity challenges. The challenges we mention are low scale issues likely related to individual cases, but not far from the future, we need to tackle organized state-sponsored cyber intrusions that need a more robust and collective response. Whether it is a national strategy to deter nation-states or a strategy on preventing cyber criminal activities, we need an evidence-based approach. As a nation, we need to have data and monitor and understand patterns across criminal activities across Sri Lanka. An evidence-based approach will inform law enforcement on criminal activity trends to be better prepared with tools and techniques.

A well-defined strategy involved training law enforcement personnel, introducing a framework on using proper tools and techniques so that even a law enforcement officer in remote villages know how to do it without depending on high tech tools only available in Colombo. Planning and deciding what to train and the nature of tools and techniques that we should be adapting should be entirely dependent on current situations, past data, and future trends; hence, it should be based on data collected and processed across Sri Lanka.

Conclusion

We believe it is high time that necessary stakeholders will amend the current regulations to comply with the latest threat landscape and technologies. We believe the lack of proper tools and legal frameworks will make investigations harder and work as an incentive for criminals. We believe that this work will provide the necessary context for a much need dialog to discuss the future of the legal framework, how to safeguard people's privacy, and, most importantly, how to speed up investigations with proper tools.

References

Archibong, I., 2018. *A Platform Update.* [Online] Available at: https://about.fb.com/news/2018/07/a-platform-update/
[Accessed 22 07 2020].

Bearman, J. & Hanuka, T., 2015. *The Untold Story of Silk Road, Part 1.* [Online] Available at:

https://www.wired.com/2015/04/silk-road-1/ [Accessed 23 July 2020].

Catherine Jasserand, 2018. Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?. *European Data Protection Law Review,* 4(2), pp. 152-167.

David Goldschlag, Michael Reed & Paul Syverson, 1999. Onion routing. *Communications of the ACM,* 42(2).

Desmond Upton Patton, et al., 2014. Social media as a vector for youth violence: A review of the literature. *Computers in Human Behavior,* Volume 35, pp. 548 - 553.

Europe, C. o., 2001. *Convention on Cybercrime.* [Online]
Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention
[Accessed 22 07 2020].

Feiner, L., 2020. *Apple refuses government's request to unlock Pensacola shooting suspect's iPhones.* [Online]
Available at: https://www.cnbc.com/2020/01/14/apple-refuses-barr-request-to-unlock-pensacola-shooters-iphones.html
[Accessed 23 07 2020].

Grace Chi En Kwan & Marko M. Skoric, 2013. Facebook bullying: An extension of battles in school. *Computers in Human Behavior,* 29(1), pp. 16-25.

Investigation, F. B. o., n.d. *Nigerian Letter or "419" Fraud.* [Online]
Available at: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud
[Accessed 24 07 2020].

Jan H.Kietzmann, Kristopher Hermkens, Ian P.McCarthy & Bruno S.Silvestre, 2011. Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons,* 54(3), pp. 241-251.

Jardine, E., 2015. *The Dark Web Dilemma: Tor, Anonymity and Online Policing.* Virginia Tech, s.n.

Jessa Lingel & Adam Golub, 2015. In face on Facebook: Brooklyn's drag community and sociotechnical practices of online communication.. *Journal of Computer-Mediated Communication,* 20(5), pp. 536-553.

Joshua Brunty & Katherine Helenek, 2012. *Social Media Investigation for Law Enforcement.* s.l.:Routledge.

Joshuah Bearman & Tomer Hanuka, 2015. *The Untold Story of Silk Road, Part 1.* [Online]
Available at: https://www.wired.com/2015/04/silk-road-1/
[Accessed 23 07 2020].

Karabiyik, U. et al., 2016. A Survey of Social Network Forensics. *Journal of Digital Forensics, Security and Law (JDFSL),* Volume 11, pp. 55-128.

Kathryn C. Seigfried-Spellar & Sean C. Leshney, 2016. Chapter 4 - The intersection between social media, crime, and digital forensics: #WhoDunIt?. In: J. Sammons, ed. *Digital Forensics.* Boston: Syngress, pp. 59 - 67.

KEMP, S., 2020. *DIGITAL 2020: SRI LANKA.* [Online]
Available at: https://datareportal.com/reports/digital-2020-sri-lanka
[Accessed 22 07 2020].

Krombholz, Katharina, Merkl, Dieter & Weippl, Edgar, 2012. Fake identities in social media: A case study on the sustainability of the Facebook business model. *Journal of Service Science Research,* Volume 4.

Mirjana Gavrilovic Nilsson, Kalliopi Tzani Pepelasi, Maria Ioannou & David Lester, 2019. Understanding the link between Sextortion and Suicide. *International Journal of Cyber Criminology,* 13(1), pp. 55-69.

Narayanan, A. & Shmatikov, V., 2009. *De-anonymizing Social Networks.* Washington, DC, USA, IEEE Computer Society.

Nova, F. F. et al., 2018. *Silenced Voices: Understanding Sexual Harassment on Anonymous Social Media Among Bangladeshi People.* s.l., ACM, p. pages 209–212.

PARLIAMENT OF THE DEMOCRATIC SOCIALIST REPUBLIC OF SRI LANKA, 2007. *COMPUTER CRIME ACT, No. 24 OF 2007,* Colombo: THE GOVERNMENT PUBLICATIONS BUREAU.

Paullet, Karen & Pinchot, Jamie, 2012. *Cybercrime: The Unintentional Effects of Oversharing Information on Facebook.* s.l., s.n.

Rachel L.Frost & Debra J.Rickwood, 2017. A systematic review of the mental health outcomes associated with Facebook use. *Computers in Human Behavior,* Volume 76, pp. 576-600.

Reporter UCA News, 2020. *Facebook sorry for role in Sri Lankan riots.* [Online] Available at: https://www.ucanews.com/news/facebook-sorry-for-role-in-sri-lankan-riots/88037 [Accessed 23 07 2020].

Scott, J. D., 2017. Social Media and Government Surveillance: The Case for Better Privacy Protections for Our Newest Public Space. *Journal of Business & Technology Law ,* 12(2).

Senaratne, N., 2020. *The Growing Need for Privacy and Data Protection in Sri Lanka.* [Online] Available at: https://www.ips.lk/talkingeconomics/2020/01/13/the-growing-need-for-privacy-and-data-protection-in-sri-lanka/ [Accessed 23 07 2020].

Shirky, C., 2011. The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs,* 90(1), pp. 28-41.

SLCERT|CC, 2019. *Annual Activity Report 2019,* Colombo: Sri Lanka Computer Emergency Readiness Team | Co-ordination Center.

SON, J., 2012. *Social Network Forensics: Evidence Extraction Tool Capabilities.* AUT University, New Zealand: Design and Creative Technologies in the school of Computing and Mathematical Sciences.

Szoka, Berin & Thierer, Adam, 2009. COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech. *SSRN Electronic Journal.*

TRCSL, 2020. *Statistics,* Colombo: Telecommunications Regulatory Commission of Sri Lanka.

UNCTD, n.d. *Data Protection and Privacy Legislation Worldwide.* [Online] Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx
[Accessed 23 07 2020].

Zaman, R. & Hassani, M., 2019. *Process mining meets GDPR compliance: the right to be forgotten as a use case.* Aachen, Germany, s.n.

Acknowledgment

We would like to show our gratitude to Criminal Investigation Department of Sri Lanka Police for their cooperation during the research study.

Author Biographies

Laksiri Geethal is a Senior Superintendent of Police and Director Police Tourist Division. He obtained his MSc. in Information Security from University of Colombo School of Computing. He has a postgraduate diploma in Criminology and Criminal Justice from University of Sri jayawardhanapura and trained on Darknet and Darkweb investigations at Interpol Training Center, Singapore. He is a lecturer in Police Academy (Cybercrime and cybersecurity). His research interests include Digital Forensics, Cybersecurity and Law, Criminal Investigations.

Kasun De Zoysa is a senior lecturer at University of Colombo School of Computing (UCSC). He obtained his Ph.D from the Stockholm University, Sweden. He is an advisor to the Sustainable Computing Research Group and Centre for Digital Forensic attached to UCSC. He teaches Digital Forensics, Cryptography, Cybersecurity, Information Security at UCSC. He conducts lectures and trainings on Information Security both locally and internationally. His research interests include Digital Forensics, Cybersecurity, Cyptographic Systems, Information Security.

Kenneth Thilakarathna is a lecturer at University of Colombo School of Computing (UCSC). He obtained his M.Phil from UCSC. He is an advisor to the Sustainable Computing Research Group. He teaches Network Security, Digital Forensics, and Security in Governence at UCSC. His research interests include Digital Forensics, Cybersecurity, Network Security, and Security in Governence.

Primal Wijesekera is a research scientist affiliated with International Computer Science Institute and Electrical Engineering and Computer Science Department in University of California, Berkeley. He obtained his Ph.D from the University of British Colombia. He is an advisor for Sustainable Computing Research Group. He teaches Mobile Forensics and Privacy in the masters programs at UCSC. His research interests include Mobile Forensics, Cybersecurity, Privacy, Fake News, Understanding Hackers and Permission systems in general.

Chamath Keppitiyagama is a senior lecturer at the Universtiy of Colombo School of Computing (UCSC). He obtained his Ph.D from the University of British Colombia. He is an advisor to the Sustainable Computing Research Group. He teaches Digital Forensics, Cryptography, Operating Systems and Computer Networks at UCSC. His research interests include Cryptography, Computer Networks, Distributed Systems, and Operating Systems.