THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

STANDALONE SOFTWARE REGULATION IN DEMOCRATIC COUNTRIES

RESEARCH FELLOWS
Andrew Dooley
Yiqi Huang

SENIOR RESEARCH FELLOWS
Cale Fuoco

FACULTY LEAD
Jessica L. Beyer

GLOBAL RESEARCH GROUP
AUGUST 2022

This report is a product of the Global Research Group Program in the Henry M. Jackson School of International Studies at the University of Washington. The Global Research Groups match teams of top-achieving Jackson School students with private and public-sector organizations seeking dynamic, impactful, and internationally-minded analyses to support their strategic and operational objectives.

For more information about the Global Research Groups please visit our website at http://jsis.uw.edu/grg/

Standalone Software Regulation in Democratic Countries

Global Research Group, Jackson School of International Studies

August 2022

Synopsis
In order to understand the regulatory landscape related to standalone software, this report examines the landscape of standalone software regulation across 19 democratic countries and the European Union. Surprisingly, we found very few regulations specific to standalone software. The majority of the regulations we analyzed did not explicitly mention standalone software, but addressed software in general. Despite this, we determined that, in some cases, the regulation of software generally was being broadly applied to cover standalone software.

Research Fellows
Andrew Dooley
Yiqi Huang

Senior Research Fellow
Cale Fuoco

Faculty Lead
Jessica L. Beyer

Contact: Jessica L. Beyer, jlbeyer@uw.edu

Table of Contents

Executive Summary

The regulation of standalone software cybersecurity in democratic countries is often difficult because standalone software can be purchased from anywhere and downloaded, which makes it more challenging to regulate than a physical product. In order to understand the regulatory landscape related to standalone software, this report examines the landscape of standalone software regulation across 19 democratic countries and the European Union. Surprisingly, we found very few regulations specific to standalone software. The majority of the regulations we analyzed did not explicitly mention standalone software, but addressed software in general. Despite this, we determined that, in some cases, the regulation of software generally was being broadly applied to cover standalone software.

Through the analysis of existing regulations of standalone software, we discovered regulation of standalone software within the following policy categories:

- International trade agreements
- Cybercrime regulation
- App store regulations
- Mandatory vs. voluntary standards
- Software requirements for regulated sectors

The report discusses each of these five policy categories at the region level so as to identify and articulate patterns in standalone software regulation across states. The regions and countries included are:

- Africa: Ghana, Kenya, Mauritius, Nigeria, South Africa, Zambia
- Americas: Brazil, Mexico, Panama, United States
- Asia: Australia, India, Japan, New Zealand, Philippines, Republic of Korea, Singapore, and Israel
- Europe: European Union, United Kingdom

Each policy category includes a discussion of potential barriers, or speed bumps, for consumers and manufacturers in obtaining or possessing the software and the enforcement mechanisms in place for regulations. The attached spreadsheet contains the entire database of regulations that we gathered and is organized by regulation.

We identified best practices in the regulation of standalone software through close examination of our five policy categories. These best practices include:

- Requiring labeling and certifications for standalone software products.
- Sanctions for utilizing standalone software to commit cybercrimes.
- Special security requirements on standalone software applications.
- Prohibition on the sale of security standalone software that may weaken a country's position or overall advantage.

Research Methods

In order to formulate a model of best practices for the regulation of cybersecurity of standalone software, we examined standalone software regulation within four regions – Africa, the Americas, Asia, and Europe. Within these regions, researchers identified 26 countries that were democracies with the state capacity to regulate technology. Researchers examined the regulatory context of each of these 26 countries plus the European Union, and narrowed the list of countries based on the presence of regulation that touched on standalone software. The final list consists of 19 countries and the European Union. The regions and countries included are:

- Africa: Ghana, Kenya, Mauritius, Nigeria, South Africa, Zambia
- Americas: Brazil, Mexico, Panama, United States
- Asia: Australia, India, Japan, New Zealand, Philippines, Republic of Korea, Singapore, and Israel
- Europe: European Union, United Kingdom

Researchers cast a wide net, looking at any regulation within each of these entities that might touch on software. To do this, they reviewed academic articles, official government websites and databases, legal databases, and consulted with the Microsoft team. The team initially gathered 89 regulations across these countries and the EU. Figure 1 illustrates the initial list of regulations distributed by country.

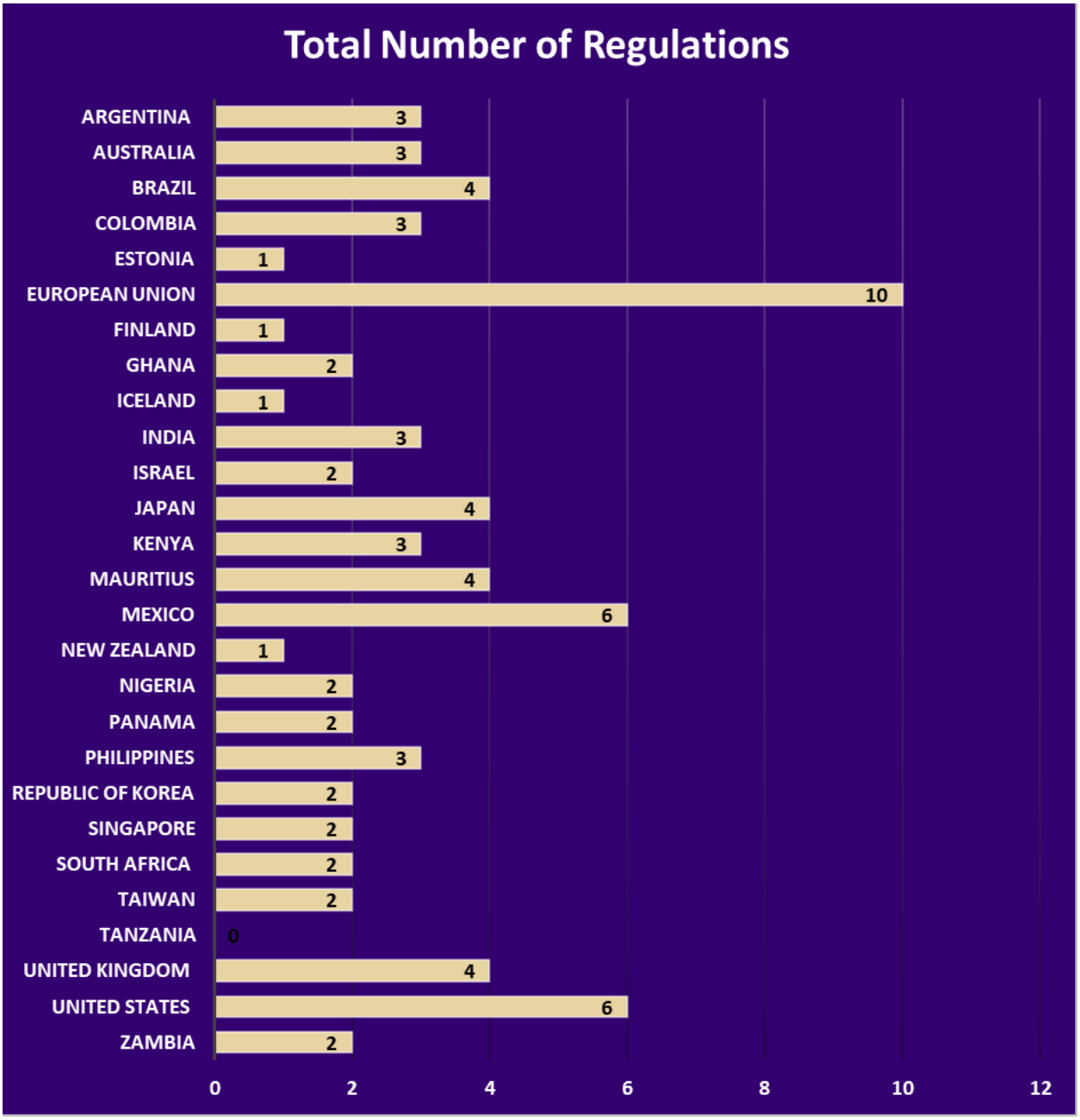

Figure 1: Initial Number of Regulations by Country

After aggregating these 89 regulations, the filtered out those that did not regulate standalone software specifically. The final list included a total of 40 regulations. Figure 2 illustrates the final list of regulations by governing actor.

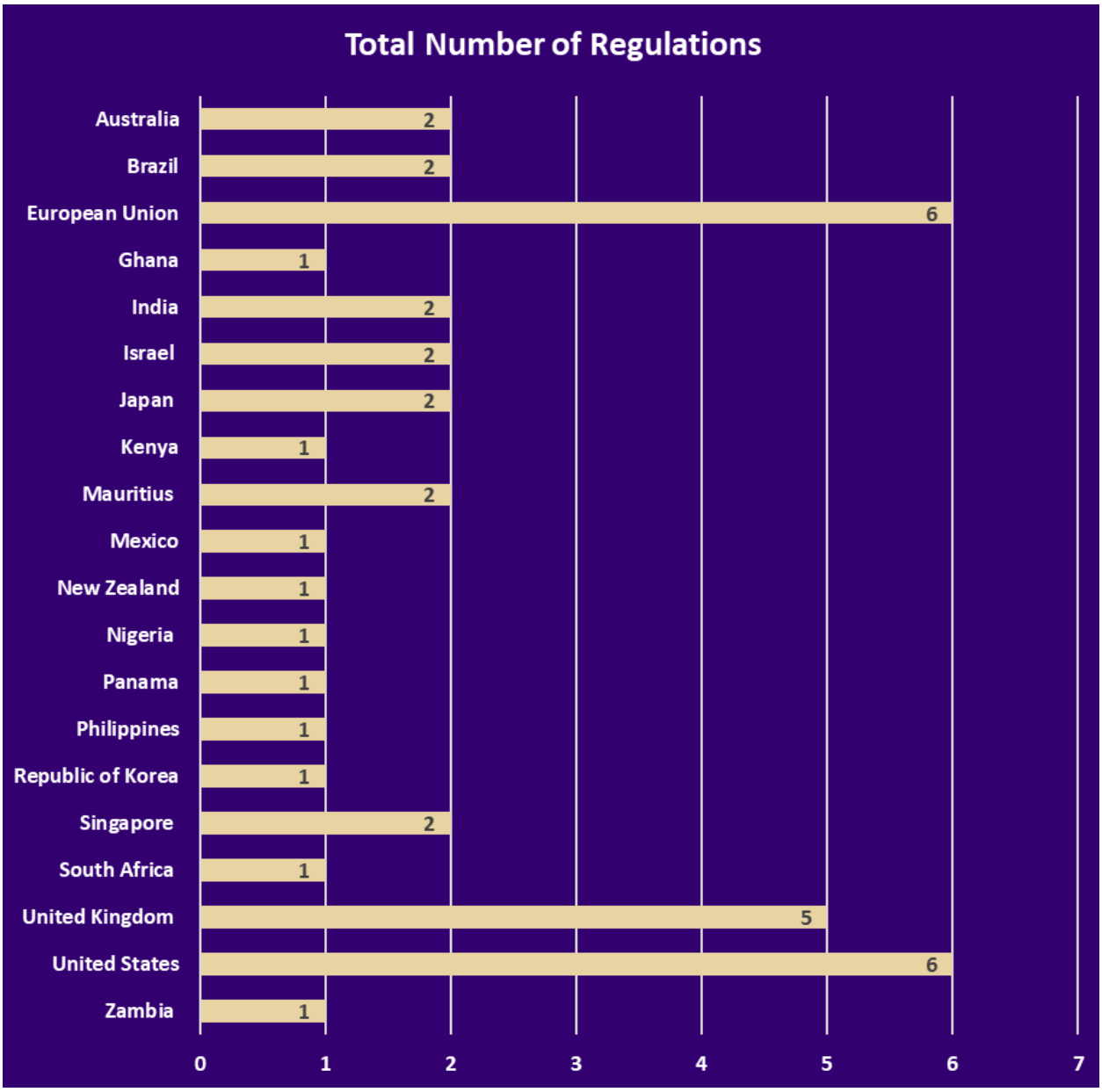

Figure 2: Final Number of Regulations by Country

From this list of regulations, the team generated the following policy categories: (1) international trade agreements, (2) cybercrime regulation, (3) app store regulations, (4) mandatory vs. voluntary standards, and (5) software requirements for regulated sectors.

International trade agreements are international treaties, agreements, accords, or conventions that include provisions that regulate standalone software. *Cybercrime regulations* outlaw the dissemination, creation, and distribution of tools that facilitate cybercrime and focus on the outcomes of digital crimes. *App store regulations* focus on the governance of application stores – which are online centralized digital platforms that provide software for purchase and download. Consumers can download apps from different publishers around the world to their devices. App store regulations require that specific applications, such as malicious or malware prone

applications, be removed from their respective stores. *Mandatory versus voluntary standards* are a combination of law and standards that provide guidance but are not legally binding. Mandatory standards are laws and failure to follow them could result in legal penalties and liability. However, voluntary standards are rules, guidance about a product or a process. Both provide guidance for software development and mandatory guidelines for cybersecurity certifications of ICT products, services, and processes. *Software requirements for regulated sectors* are standalone software regulations in different sectors and industries. Most of the regulation researchers discovered relate to software-as-a-medical-device and mobile banking and payments.

In addition to finding all regulations that fit within these categories, researchers also looked for enforcement mechanisms as well as "speed bumps" that would prevent consumers from acquiring the standalone software and would prevent manufacturers from offering the software for sale. Researchers also examined enforcement mechanisms, including what constituted enforcement and what actor was responsible for it. Researchers also kept track of attributes distinct to each country that might shape how regulations were adopted or made – such as major trading partners or major domestic industries.

Finally, the team analyzed each regulation to discern if there were any features of the regulation that could be considered best practices for standalone software or that other governments may want to emulate. Tied to this, researchers identified any obvious limitations of regulations.

International Trade Agreements

Generally, international trade agreements do not include consideration of the regulation of standalone software. While we examined multiple major international agreements to ascertain whether they included regulation of standalone software, we found that only two did: the Budapest Convention on Cyber Crime and the Malabo Convention. We also examined other international institutions, such as the WTO, but found no other international agreements applicable to standalone software regulations.

Budapest Convention on Cyber Crime

The Budapest Convention covers a variety of topics and issues related to cybercrime and within this material, concerns about software and data relate to questions of standalone software. The Budapest Convention on Cyber Crime was drafted in 2001 by the Council of Europe and then enacted in 2003 (Budapest Convention, 2003). The Convention sets forth general principles to increase cooperation in the area of cybercrime.

The Budapest Convention addresses standalone software regulation under Titles 1 and 2. Title 1 focuses on offenses against the confidentiality, integrity, and availability of computer data and systems. This category sets out to legally define a subset of cybercrimes covering illegal access and interception, data and system interference, computer-related fraud, and misuse of devices. Title 2 refers to computer-related offenses. This title covers crimes relating to computer-related forgery and fraud by use of any means, including software. While there is no explicit mention of standalone software in these two titles, it can be inferred that software regulations cover standalone software because cybercrime is not bound by a single device or operating platform.

The provisions set out in this convention do not create an international body tasked with enforcing cybercrime laws or norms. Rather, it establishes that the burden of enforcement lies with domestic governments (Budapest Convention, 2003). Since this Convention's activation, the total number of states ratifying it is 66 and 16 have been invited to accede or join (Council of Europe, 2022).

The Malabo Convention

The African Union's Malabo Convention tackles the issue of cybercrime and the problems faced by the Union. Several provisions seek to criminalize the usage of standalone software facilitating cybercrimes and attacks. Since its adoption in 2014, eight African Union members have ratified it and 14 have signed it (Malabo Convention, 2014). One of the objectives of this convention is to encourage member states to develop criminal statutes to combat cybercrime.

This Convention addresses the issue of criminals using standalone software to commit cybercrimes. In Chapter III Section II Article 29 (1), cybercrimes are defined and categorized into four distinct categories: attacks on computer systems, computerized data breaches, content related offenses, and offenses relating to electronic message security measures (Malabo Convention, 2014). It must be noted that software is not explicitly mentioned in this particular article. However, the relationship to software can be inferred under Article 29 (1), focused on

attacks on computer systems, and Article 29 (2), focused on computerized data breaches (Malabo Convention, 2014). Further, the broad applicability of software entails the inclusion of standalone software products and services that would facilitate such cyberattacks. While there is no mention of standalone software connections can be drawn between cyberattacks and the standalone software that facilitates it.

Cybercrime Regulations

Generally, cybercrime refers to a criminal activity involving computational devices or taking place over the internet. Barring definitions of cybercrime in international treatises, what constitutes a cybercrime will vary around the world, and with it the approach to preventing such criminal activities. Standalone software has begun to receive recognition as a tool in need of regulation in this regard; criminalization of malicious software is just one example that many countries have begun to implement.

Across the 19 countries we identified, there are two primary routes countries take in their efforts to curb cybercrime in regards to standalone software, assuming that the country has already recognized and defined cybercrimes. First, countries target the dissemination of tools that facilitate cybercrimes by making the creation and distribution of said tools illegal. Second, countries focus on the outcomes of digital crimes such as financial loss or theft. Countries that use the second approach may not have a unique agency or institution(s) responsible for cybersecurity and so delegate these responsibilities into respective sectors that could be targeted in cyberattacks. Finance, administration, healthcare, and IT are some of the potential areas cybercrime-adjacent policy may apply to. Both of the aforementioned approaches target cybercrime broadly and utilize agendas that may not rely on standalone software regulation explicitly; the vast majority of cybercrime regulation does not specifically target “standalone software” and that was a significant challenge in conducting this research.

Africa

African countries have made great strides in addressing the issue of standalone software as a tool to facilitate cybercrime. Several noticeable patterns have been found in the various cybercrime legislation, such as providing legal definitions for specific crimes and restrictions on hacking software tools and hardware. Many of the countries have referred to their domestic penal codes for those convicted of cybercrimes. We focused on restrictions and illegality of standalone software that would enable hacking, unauthorized access, interception, destruction, or other nefarious activities. It must be noted that while African cybercrime laws do not explicitly mention standalone software, the broad applicability for the prohibition of software applies to standalone software.

There is a noticeable difference in methods used to tackle the issue of cybercrime. The first approach focuses on the use of the standalone software and intent. The second approach focuses on the production, sale, distribution, and procurement of hacking software. In Mauritius, the Computer Misuse and Cyber Crimes Act takes on the first approach. This act expressly outlaws the use of technical means to intercept or cause interception without authorization from a computer system. Intentionally injuring the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data (Computer Misuse and Cyber Crimes Act, 2003). The act prevents people from utilizing software but does not prevent them from procuring or possessing it. According to the act, the Mauritius Ministry of Information and Communication Technology is tasked with the enforcement (Computer Misuse and Cyber Crimes Act, 2003). In addition, the Ministry of Justice will have the obligation to prosecute those accused of committing such crimes prescribed in this act.

Consistent with the second approach focusing on the production, sale, distribution, and procurement of hacking software, South Africa's Cybercrimes Act of 2020 addresses the same issues. This law however takes a slightly different approach in that it tackles the problem of misusing a computer. It states that it is unlawful to use computer resources, programs, and software to engage in online criminal activity defined in this act (Cybercrimes Act of 2020, 2020). Moreover, use of software or hardware tools are prohibited and unlawful. Thus, the law includes prohibitions on obtaining these software tools and hardware as well as prohibitions for those who develop and manufacture products. According to this law, the South African National Police and the Ministry of Justice are tasked with enforcement. Nigeria has also adopted this approach in its Cyber Crime Act of 2015. The Nigerian law makes it unlawful to produce, supply, adapt, manipulate, or procure for use of import, export, distribute, offer of sale or otherwise make available software that facilitates unauthorized access to personal/security information (Cyber Crime Act of 2015, 2015).

Kenya's Computer Misuse and Cyber Crimes Act utilizes similar wording to that of previously aforementioned countries. This law criminalizes the possession, distribution, or production of hacking software tools, hardware, and devices. Prohibitions exist for those who want to obtain, manufacture, and develop hacking software and tools. The Kenyan National Police Service acts as the enforcement mechanism for the crimes laid out.

Zambia's recent legislation on cybercrimes also takes on this second approach. It criminalizes the use of software tools and hardware to facilitate prescribed cybercrimes (Cyber Security and Cyber Crimes Act, 2021). It outlawed the sale, production, procurement for use of imports, exports, distributes or make available computer programs (software) to commit a cybercrime. This act creates barriers for those who want to obtain, distribute, manufacture, and develop software that would facilitate the prescribed cybercrimes. The Zambian Ministry of Justice is tasked with the enforcement of this act and prosecuting the crimes allegedly committed.

Americas

Countries in the Americas vary immensely in their development of cybercrime enforcement mechanisms and recognition of standalone software as a tool in need of regulation. Many have begun the process of developing a cybersecurity agenda, and nations such as Canada and the US can be said to lead global cybersecurity efforts. Panama, Colombia, and Argentina are all in the process of implementing cybersecurity agendas, though Argentina lacks official legislation to codify cybercrimes. The United States likely has the most complex and comprehensive cybersecurity regulations in place of any country in this region, and when we look to the region as a whole it may appear as an outlier. Standalone software is most often regulated through applications of already existing legislation, or via data security and personal privacy laws.

For example, Brazil's Penal Code 154, which was updated in 2021 and became a new law named Law No. 14,155, increases the punishment for whoever invades someone else's computer device, whether connected to the internet or offline, in order to obtain, tamper with, or destroy data or information without the express or tacit authorization of the user of the device, or to install vulnerabilities to obtain an unlawful advantage. The code also makes note of theft through the

use of computer programs, and the penalties are increased if a server outside of Brazil is discovered to have been used in the attack. Penalty for those found to violate this penal code will range from three months imprisonment and a fine to up to one year. As this focuses on the usage of standalone software and not its distribution, roadblocks to acquiring standalone software are beyond its scope.

In another example, the American Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries is itself a reaffirmation of Executive Order 13873 of May 15, 2019, which was brought forth due to allegations that TikTok was providing user data – specifically that of active military service members – to parent company ByteDance in China. The Executive Order cites the International Emergency Economic Powers Act, the National Emergencies Act, and Section 301 of Title 3 in its decision to force TikTok to immediately suspend data sharing, with a seven-day deadline, and suspension in the United States. Enforcement meant that TikTok would no longer be allowed on American app stores, causing any who might want to download the application to need either a Virtual Private Network (VPN) or to be in a location not under US jurisdiction (The American Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries, 2021).

In Colombia, the Colombian Constitution's Articles 15 and 20 codify the right to privacy and freedom of speech respectively, with 15 also providing protections to data security. These articles state that all individuals have the right to personal and family privacy and to their good reputation, and the state has to respect them and to make others respect them. Similarly, individuals have the right to know, update, and rectify information collected about them in data banks and in the records of public and private entities. The usage of software to misappropriate one's data will be considered a violation of the respective articles. Violation of these articles will likely result in criminal penalty, though the constitution makes no note of what those may be. As this regulation applies only to standalone software in the context of it being used to steal information, it will likely not create any roadblocks for a person looking to download any given standalone software (Colombian Constitution, 1991).

Asia

Among the eight Asian countries that we analyzed; most countries have enacted laws against cybercrime. Half of these countries referred to the penalties imposed by their domestic criminal codes on those convicted of cybercrime. The most frequently included in these codes are criminal punishments for those who distribute, sell, or offer to sell hardware, software, or other tools used to commit cybercrime and those who possess or use hardware, software or other tools used to commit cybercrime. Although the regulations do not explicitly mention standalone software, the regulation of software can be assumed to include the regulation of standalone software as a subset. Examples include, Japan's Penal Code, Article 168-2 and 168-3; Philippines' Republic Act No.10175; Australia's the Criminal Code Act Section 478; New Zealand's the Criminal Act, section 249-252.

The remaining countries have especially formulated laws against cybercrime in addition to their criminal codes, such as Singapore's the Computer Misuse Act; India's the IT Act, section 43; Israel's Computers Law. The main purpose of these laws is also to crack down on a series of

activities such as using malicious software (standalone software as a subset) to invade computer networks, steal data, introduce and spread viruses through computer networks, and destroy computer networks, programs, and information without authorization.

Europe

The technological developments in Europe have caused governments to address issues of cybercrime and cyberattacks. Common patterns found in the European Union and in the United Kingdom have been developing a legal framework to criminalize and punish those who commit cyberattacks, including when actors use standalone software tools and hardware to facilitate such attacks. The European Union's Directive 2013/40 develops a comprehensive framework that sets out to legally define various types of cyberattacks. For example, it covers crimes such as: illegal access to information systems, illegal interference with systems and data, illegal interception, and tools used for committing offenses (Directive 2013/40, 2013). While this act does not explicitly mention standalone software, it can be presumed that mentions of software should be considered an umbrella term to incorporate standalone software. The European Union has creates barriers for people who want to utilize hacking software for cybercrimes or for the purposes to commit a cyberattack. According to this act, the EU Commission delegates enforcement of this directive to national governments and their relevant agencies (Directive 2013/40, 2013).

The United Kingdom's Computer Misuse Act of 1990 is structured differently than that of the EU. This act from 1990 sets out to criminalize offenses or attacks against computer systems such as hacking or distributed-denial-of-service attacks (Computer Misuse Act, 1990). While this act does not mention standalone software, it can be inferred that the means to facilitate an attack would incorporate standalone software as a tool. This act creates prohibitions for those who want to utilize the software for nefarious purposes. It must be stated that this act does not prohibit the production of or the sale of hacking software. The United Kingdom's Ministry of Justice and relevant law enforcement agencies are tasked with the enforcement of this act. It was difficult to pinpoint the exact law enforcement agency or the relevant cabinet ministry tasked with enforcement of this act.

App Store Regulations

An application store (app store) is an online centralized digital platform where software programs are made available for procurement and download. Consumers can acquire apps from different publishers around the world downloaded to their devices. Two of the world's largest app stores are Apple's App Store and Google's Google Play. Outside of China, Apple's App Store and Google Play control more than 95 percent of the app store market share through iOS and Android, respectively. In Africa, the Americas, Asia, and Europe, there are very few regulations of app stores as related to standalone software. Instead, the regulations for app stores fall mainly into two camps: (1) antitrust legislation meant to ensure the fair operation of digital platforms or (2) prohibitions against specific applications, such as malicious or malware prone apps.

Africa

The African region has made great strides in developing regulations on standalone software in various sectors and contexts. We see this in cyber rime norms, international agreements, the financial sector, and public and private partnerships. Unfortunately, after careful research on app store regulations under the purview of software regulation, we have not found substantial evidence to indicate the African region has any regulation of app stores as a venue for standalone software. For the context of Africa, it can be surmised from a majority of their software regulations target cybercrime and the financial sector. App store regulation under software has not been developed. However, developments in the app store privacy and data governance and protection are being legislated on and regulated.

Americas

In the Americas, little to no regulation exists on app stores themselves from a standalone software perspective. The only contexts in which regulations were found targeting app stores was in regards to antitrust legislation or when a specific application was targeted for removal for security reasons. Some examples include: Brazil's Petition 9935 against Telegram which gave the company one week to remove the accounts of Jair Bolsonaro from their service or be immediately suspended from all App Stores in Brazil and the US Executive Order mandating TikTok halt data sharing with ByteDance. App Stores do not appear to be given a unique regulatory framework in the Americas (Petition 9935, 2022).

Asia

Unfortunately, there are no relevant app store regulations in Asia concerning standalone software. The conversation happening in this region is more focused on antitrust issues and fair business practices.

Europe

Removing app store regulations focused on privacy and data protection regulation from consideration, the United Kingdom has proposed several key bills that cover app store standalone software requirements. The App Security and Privacy Intervention Proposal (2020) requires app store operators to remove malicious or malware prone apps from its stores and require standards in app security. This proposal would include standalone software from mobile applications. Any platform the infected or malware prone application is on would be removed from the market (App Security and Privacy Intervention, 2020). This bill will also consider financial incentives to promote and motivate the private sector to comply with the given regulations. App developers and platform providers must continuously monitor their systems and implement security patches and filter apps infested with malware. Barriers for app download or use appear for people when standalone mobile application software does not comply with the regulatory standards and security requirements. There may be regulatory sanctions imposed that may inhibit people from downloading the application on all digital marketplaces and stores. The agency responsible for the enforcement of this proposal is the Department for Digital, Media, Culture and Sports and to ensure compliance among the app developers operating on the open market.

In addition, the United Kingdom proposed regulations on security requirements for connectable products. The Product Security and Telecommunications Infrastructure Proposal (2022) contains security requirements for connectable products and allows for the Secretary of State for Digital, Media, Culture, and Sports to specify what security requirements are for connectable products and standards for manufacturers and distributors. While this act does not explicitly mention standalone software, the security requirements for the connectable products would include standalone software. The standalone software requirements for the connectable products whether through the internet or a network must be met. The manufacturers and distributors must meet pre-market requirements in order to be authorized to sell their products (Product Security and Telecommunications Infrastructure, 2022). The requirements must be self-assessed by the manufacturer and distributor on their products before bringing them to market. A statement of compliance must be made on the product by the manufacturer and distributor (Product Security and Telecommunications Infrastructure, 2022). These requirements create a barrier for both consumers and manufacturers. Consumers would not be able to purchase products that do not meet the regulatory requirements laid out in this proposal. Furthermore, companies that fail in certifying their products will receive regulatory penalties as prescribed in this proposal. The agency tasked with enforcement is the United Kingdom’s Department for Digital, Media, Culture, and Sports and to ensure compliance with regulatory standards.

Mandatory vs. Voluntary Standards

Mandatory versus voluntary standards include both legally binding law and standards that provide guidance but are not legally binding. Failure to abide by mandatory standards could result in legal penalties and liability. However, voluntary standards are rules or guidance about a product or a process. Both provide guidance for software development and mandatory guidelines for cybersecurity certifications of ICT products, services, and processes. In Africa and Asia, there are few mandatory and voluntary standards for standalone software. However, there are relevant regulations in the Americas and Europe. In the Americas, the most prominent voluntary is the creation of standardized certification and guidance indicators for software development. In Europe, the European Union Cybersecurity Act provides a common framework for ICT products and services, and provides guidance on cybersecurity certification for ICT products, services, and processes.

Africa

There are few regulations on mandatory and voluntary standards concerning standalone software on the African continent. However, there are some exceptions. For instance, Ghana enacted the Cybersecurity Act of 2020 that sought to create a voluntary certification scheme and cybersecurity authority (Cybersecurity Act of 2020, 2020). Businesses will have the option to participate in the voluntary industry standards. These standards shall be established by an industry forum and adopt subsequent initiatives. Companies that meet specific requirements and successfully pass rigorous testing of software and penetration testing receive its certification. Another major provision in this act creates a Cyber Security Authority that can implement standards for cybersecurity of hardware and software engineering (Cybersecurity Act of 2020, 2020). Although this act does not expressly mention standalone software, the regulation of the software would entail it.

Americas

In the Americas voluntary standards exist, most notably in the creation of standardized certifications and guidance metrics for software development. The Standardization and Certification Enterprise, originally started as a non-profit organization by the Mexican government to increase interest in their software development sector, saw success. The Standardization and Certification Enterprise has branched into many different fields for its certifications and is now operating in multiple countries, but since being acquired by QIMA – a for profit company – little can be said about the plans for the future of the organization. It has partnered with the Mexican Government in the past to create frameworks for the standardization and certification of standalone software, as shown with their IT Technology - Software Evaluation products (Standardization and Certification Enterprise, 2006).

Asia

In Asia, we found no regulations on mandatory and voluntary standards concerning standalone software.

Europe

In Europe, there are mandatory guidelines for cybersecurity certifications of ICT products, services, and processes. The European Union Cybersecurity Act (2019) seeks to provide a framework for ICT products and services. This EU-wide certification provides uniformity, a comprehensive set of rules, technical requirements, standards, and procedures. While this new framework does not explicitly mention standalone software, it can be inferred that the requirements for ICT products would have broad applicability to it. Industry will be required to comply with the security regulations for the standalone software of ICT products (Cybersecurity Act of 2019, 2019). The European Agency for Cybersecurity acts as the enforcement mechanism for this act and monitors compliance.

Software Requirements for Regulated Sectors

Standalone software requirements for regulated sectors cover a multitude of areas. Depending on the region, priorities vary in how governments regulate each sector pertaining to standalone software. The African region sees strong regulation on the financial and banking sectors. The government of Mauritius in particular has developed strong and efficient regulations for mobile banking applications. In Europe, we see extensive regulation on the financial sector and e-commerce. In the Americas, regulations focus on critical software such as aviation software and software as a medical device. In Asia, regulation focuses on the medical field and healthcare.

Africa

The African continent does not have extensive regulation of software requirements for regulated sectors. However, Mauritius has recently developed key standalone software regulation for the financial sector. The Guideline on Mobile Banking and Mobile Payments System (2013) provides an overview of software requirements for the mobile banking applications. Further, it requires that mobile banking applications have monitoring software to detect unauthorized access. It also requires the mobile banking application servicer to implement triple data encryption standard or AES to its transactions processes (Guideline on Mobile Banking and Mobile Payments System, 2013). While this act does not explicitly mention standalone software, it can be presumed that the regulation of software applies to standalone software. The mobile applications are not bound to one platform nor to any single device, thus the regulation of the software applies broadly. What makes it distinct is that these regulations are enforced by the Central Bank of Mauritius. Prohibitions that consumers will face include if the mobile payment service providers fail to comply with the standards and requirements set by this act and by the Central Bank of Mauritius. Regulatory sanctions may be imposed that would inhibit consumers from accessing or downloading the mobile application.

Americas

In the Americas, the main sectors that require software requirements vary. In South America there are very few regulated sectors, with the exception of software-as-a-medical-device. In the United States this holds true as well, with other notable areas being aviation and federal agency use. The Federal Aviation Administration, Transports Canada, and European Union Aviation Safety Agency all mandate that aviation software abide by Federal Acquisition Regulations, and in the United States this is codified in Software Considerations in Airborne Systems and Equipment Certification Regulations. Products that fail to abide by these regulations will not be certified, which will impact their sales and likely serve as an incentive to become compliant. All the aforementioned groups require their commercial software to be compliant with the above regulations. Standalone software products to be utilized by aviation systems must also comply (Software Considerations in Airborne Systems and Equipment Certification, 2013).

The US's Department of Homeland Security maintains yearly audits of other agencies through the Federal Information Services Management Act, with agencies required to submit yearly reports of their budgets, current information systems and the software they use. The DHS may require modifications to software on the basis of efficiency or cost-effectiveness. This will not

pose a direct roadblock to consumers as this is strictly a federal mandate. If a standalone software program fails to meet the DHS's guidelines it may no longer be used, or the contract renegotiated (Federal Information Services Management Act, 2014).

Also in the US, the Encryption and Export Administration Regulations are a series of regulations enforced by the American Bureau of Industry and Security that detail the three circumstances under which exporters of cryptographic software must receive clearance prior to gaining an export license. Those circumstances are: cryptographic information security; (e.g., items that use cryptography), non-cryptographic information security (5A003); and defeating, weakening of bypassing information security (5A004) tools. Any software that additionally could be said to have such tools built in even if not its primary purpose may qualify. There are several exception types to this rule with the largest being the 'Mass Market' exception. This exception applies to items that are factory installs, aftermarket replacements, and/or are not intended to be security systems (Encryption and Export Administration, 2021). Enforcement would come in the way of revocation of an already existing export license. If the item is denied during the export license application process, then enforcement would be that item never making it to market. A consumer not in the United States would then likely have difficulties accessing it, but it would still be legal to sell in the US market.

Asia

In view of the software requirements for regulated sectors, Asian countries are mainly formulating regulations for the software of the medical equipment department. Six of the eight countries we researched have relevant laws and guidelines that have been implemented.

For instance, Japan's Pharmaceuticals and Medical Devices Act made significant updates to registration requirements and the approval process for foreign medical device manufacturers. In addition to hardware, software installed on a general-purpose computer, smartphone or other information device, used to diagnose, treat or prevent disease are treated as medical devices and subject to strict regulation under the PMD Act. Standalone software becomes a Class II device and All Class II devices' design control activities will be covered in the Quality Management System audit. (Japan Pharmaceutical and Medical Device Act-Understanding the Requirements, n.d.) Failing to meet regulatory requirements, the Pharmaceuticals and Medical Devices Agency and Ministry of Health, Labor, and Welfare will take action to enforce the policy.

South Korea's Guideline on Review and Approval of Artificial Intelligence and Big-Data based Medical Devices requires that medical device manufacturers (importers) implement and document technical measures necessary for security of medical device software (access control, de identification of personal information, data encryption and decryption, etc.) Administrative, physical, and technical matters necessary for cloud server security are managed in accordance with the Medical Service Act and the Personal Information Protection Act. This guideline is applicable to standalone software types of medical devices, to which machine-learning-based AI technology is applied, that diagnose, manage or predict diseases by analyzing medical big data. (Guideline on Review and Approval of Artificial Intelligence and Big-Data based Medical Devices, 2020) Since this guideline does not establish legally enforceable responsibilities, the

Ministry of Food and Drug Safety and Ministry of Health and Welfare will not enforce the policy.

Singapore's Regulatory Guidelines for Software Medical Devices stipulates that all software medical device manufacturers must adopt a total product life cycle approach to manage and adapt to the rapid changes, including: risk assessment, standalone software verification and validation, etc. The software version information that represents all software changes/ iteration (e.g., graphic interface, bug fixes) must be submitted to the Health Sciences Authority. The guidelines also state that a screenshot of the splash screen which displays the elements for identification, including software version number is required for standalone software labeling (Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach, 2019). Failing to meet regulatory requirements, the Health Sciences Authority will monitor and detect any failures and timely intervene.

India's Medical Device Rules require manufacturers, importers and sellers of the medical devices to obtain permission to engage in the import, manufacture, and sale of the medical devices. For devices which incorporate software or for standalone software that are devices in themselves, the software must be checked taking into account the principles of risk management, verification, and validation (Essential Principles for safety and performance of medical devices guidelines, 2018). Failing to meet regulatory requirements, the Ministry of Health and Family Welfare and civil courts will take action to enforce the policy.

Israel's Medical Equipment Law imposes a criminal prohibition on manufacturing, importing, marketing, and using medical equipment which has not been registered in the AMAR (The Medical Equipment Law, n.d.) While this regulation does not explicitly mention standalone software, the mention of software may apply to standalone software due to the ambiguity of its meaning. Failing to meet regulatory requirements, the Medical Device Division of the Ministry of Health will take action to enforce the policy.

Australia's Therapeutic Goods Act set out the requirements for inclusion of therapeutic goods in the Australian Register of Therapeutic Goods, including advertising, labeling, product appearance and appeal guidelines. If a software product is a medical device, it must be included in the Australian treatment product registration unless it is exempted in advance (Therapeutic Goods Act 1989, 2021). Although the statute does not explicitly mention standalone software, the regulation of software can be assumed to include the regulation of standalone software as a subset. Failing to meet regulatory requirements, the Therapeutic Goods Administration and civil courts will take action to enforce the policy.

Europe

Europe has been developing regulations for standalone software in sectors such as medical devices, dual-use items, payment services, and the digital markets. While these regulations are comprehensive, it is not representative of the whole of Europe. However, these developments do show governments beginning to regulate standalone software in certain sectors of industry.

The United Kingdom has developed key regulations on medical technology and the security requirements for its software. The Software As A Medical Device Regulation (2022) seeks to provide uniformity and a set of technical standards to secure medical device software. While this act does not expressly mention standalone software, regulation of software for medical devices would apply to it. The software as a medical device can be accessed through any device and mobile platform. Thus, the regulation of this software would incorporate standalone software. This act provides regulations on the duties of manufacturers pre-market and post-market surveillance of their products (Software As A Medical Device Regulation, 2022). Further, manufacturers must continuously maintain and monitor systems, install security patches, protect against third party intruders, and apps. Potential barriers consumers may face is if the software is not compliant with security standards that protect the software and mobile applications. Furthermore, manufacturers may face barriers if they are not compliant with the standards set by this act and regulatory requirements. The agency responsible for enforcement is the United Kingdom's Medicines and Healthcare Products Regulatory Agency.

The European Union on the other hand have developed specific regulations for dual-use items and digital markets. The Regulation 2021/821 (2021) of the EU sets up a community regime for the control of exports, transfer, brokering and transit of dual-use items. While this act does not explicitly state standalone software, the software regulation of dual-use items would apply to it. Dual-use items refer to products or services that have both a civilian and military use (Regulation 2021/821, 2021). Thus, the nature of the software used in this context would broadly apply to standalone software. This act provides for regulations on standalone software concerning: nuclear, aviation, naval, and missile defense. This act covers the manufacturer and developers of these dual-use products. Enforcement of this act falls under the individual Member States' domestic regulatory agencies.

The Union has imposed regulations of standalone software to the financial sector. The Payment Services Directive (2015) requires that payment service providers share their security and control mitigation framework and policies. Furthermore, they must comply with regulatory security standards and software requirements set by the European Banking Authority (Payment Services Directive, 2015). While this act does not explicitly mention standalone software, the software regulations would broadly apply to standalone software. Payment service providers operate on multiple platforms and devices thus the software requirements would assume a regulation on standalone software. According to this directive, member states are required to enforce the standards set by the EBA and respond to user complaints (Payment Services Directive, 2015). Speedbumps faced by consumers are contingent on the compliance of banks with the regulatory standards set by the EBA.

The Union has developed regulations for standalone software applications on online platforms. The Digital Markets Proposal (2020) restricts software application store platform owners from restricting equal access, regulation on the security features of software applications and software application of stores. While this act does not explicitly mention standalone software, the software regulations would broadly apply to standalone. Barriers may arise when the gatekeepers/developers are not compliant with the security requirements for mobile applications and the software they develop. The enforcement mechanism for this act is the European Commission and its relevant authorities.

Bibliography

African Union. (2014). *The Malabo Convention*. Retrieved August 24, 2022, from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

Bhawan, N. (2018). *Essential Principles for safety and performance of medical devices guidelines*. CDSCO. Retrieved August 23, 2022, from https://cdsco.gov.in/opencms/export/sites/CDSCO_WEB/Pdf-documents/medical-device/Essentialprinciples.pdf

Brazilian Penal Code. (2021). United Nations Office on Drugs and Crime. Retrieved August 24, 2022, from https://sherloc.unodc.org/cld/en/legislation/bra/codigo_penal/title_i/article_154a-b/art._154a-b.html?#:%7E:text=154%2DA%2C%20criminal%20prosecution%20can,or%20against%20public%2Dservice%20concessionaires

Constitute Project. (2022). *Colombian Constitution of 1991 with Amendments through 2015*. Retrieved August 24, 2022, from https://www.constituteproject.org/constitution/Colombia_2015.pdf?lang=en

Council of Europe. (2022). Council of Europe-Budapest Convention. Retrieved August 23, 2022, from https://www.coe.int/en/web/cybercrime/the-budapest-convention

Department of Homeland Security. (2014). *Federal Information Security Modernization Act | CISA*. Cybersecurity and Infrastructure Security Agency. Retrieved August 24, 2022, from https://www.cisa.gov/federal-information-security-modernization-act

Department of Transportation. (2013). *Advisory Circular 20–115C: Airborne Software Assurance*. Federal Aviation Administration. https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_20-115C.pdf

Digital Policy Alert. (2022). *Petition 9935*. Retrieved August 24, 2022, from https://www.digitalpolicyalert.org/event/3873-brazil-federal-supreme-court-orders-suspension-of-telegram

European Union. (2013). *Directive 2013/40*. EUR-Lex. Retrieved August 24, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013L0040&qid=1661371642585

European Union. (2019). *Cybersecurity Act of 2019*. EUR-Lex. Retrieved August 24, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1661364586854

European Union. (2021). *Regulation 2021/821*. EUR-Lex. Retrieved August 24, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821&qid=1661372020630

European Union. (2020). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)*. EUR-Lex. Retrieved August 24, 2022, from https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN

European Union. (2015). *Payment Services Directive*. EUR-Lex. Retrieved August 24, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366&qid=1661366447311

Government of Kenya, (2018). *Computer Misuse and Cybercrimes Act*. Government of Kenya. http://kenyalaw.org:8181/exist/rest//db/kenyalex/Kenya/Legislation/English/Amendment%20Acts/No.%205%20of%202018.pdf

Government of Ghana, (2020). *Cybersecurity Act of 2020*. Government of Ghana. https://csdsafrica.org/wp-content/uploads/2021/08/Cybersecurity-Act-2020-Act-1038.pdf

Government of Nigeria, (2015). *Cybercrimes Act of 2015*. Government of Nigeria. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf

Government of South Africa. (2019). *Cybercrimes Act of 2019*. South African Government. Retrieved August 24, 2022, from https://www.gov.za/documents/cybercrimes-act-19-2020-1-jun-2021-0000

Guideline on Mobile Banking and Mobile Payment Systems. (2016, June 23). Bank of Mauritius. Retrieved August 24, 2022, from https://www.bom.mu/financial-stability/supervision/guidelines/guideline-mobile-banking-and-mobile-payment-systems

Guideline on Review and Approval of Artificial Intelligence and Big-Data based Medical Devices. (2020, November). Ministry of Food and Drug Safety Medical Device Evaluation Department. Retrieved August 23, 2022, from https://www.mfds.go.kr/eng/brd/m_40/view.do?seq=72623&srchFr=&srchTo=&srchWord=&srchTp=&itm_seq_1=0&itm_seq_2=0&multi_itm_seq=0&company_cd=&company_nm=&page=1

Japan Pharmaceutical and Medical Device Act-understanding the requirements. (n.d.). BSI. Retrieved August 23, 2022, from https://www.bsigroup.com/globalassets/meddev/localfiles/en-gb/services/bsi-md-japan-market-access-brochure-uk-en.pdf

Kahn, M. (n.d.). *The Medical Equipment Law, 5772–2012*. Moshe Kahn Advocates. Retrieved August 23, 2022, from https://www.kahn.co.il/Articles-and-Media/the-medical-equipment-law-5772-2012.html#:%7E:text=The%20Medical%20Equipment%20Law%20imposes,Ministry%20of%20Health%5B2%5D.

Mauritian National Assembly, (2003). *Computer Misuse and Cybercrime Act of 2003*. Attorney General of Mauritius. https://attorneygeneral.govmu.org/Documents/Laws%20of%20Mauritius/A-Z%20Acts/C/Co/COMPUTER%20MISUSE%20AND%20CYBERCRIME%20ACT,%20No%2022%20of%202003.pdf

Mexican Standard INFORMATION TECHNOLOGY-SOFTWARE PRODUCT EVALUATION PART 1: GENERAL VISION. (2006). NYCE. Retrieved August 24, 2022, from https://nyce.org.mx/catalogodeestandaresnyce/producto/nmx-i-14598-1-nyce-2011-tecnologia-de-la-informacion-evaluacion-del-producto-software-parte-1-vision-general-cancela-a-la-nmx-i-084-01-nyce-2006/

Parliament of the United Kingdom, (1990). *Computer Misuse Act of 1990*. UK Parliament. https://www.legislation.gov.uk/ukpga/1990/18/contents

Regulatory Guidelines for Software Medical Devices – A Lifecycle Approach. (2019, December). HEALTH SCIENCES AUTHORITY. Retrieved August 23, 2022, from https://www.hsa.gov.sg/docs/default-source/announcements/regulatory-updates/regulatory-guidelines-for-software-medical-devices--a-lifecycle-approach.pdf

Reservations and Declarations for Treaty No.185 - Convention on Cybercrime. (2022). Council of Europe-Budapest Convention. Retrieved August 23, 2022, from https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0

Therapeutic Goods Act 1989. (2021). Australian Government Federal Register of Legislation. Retrieved August 23, 2022, from https://www.legislation.gov.au/Details/C2021C00376

The White House. (2021, June 9). *Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries*. Retrieved August 24, 2022, from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/

United Kingdom Department for Digital, Culture, Media, and Sports, (2022). *App Security and Privacy Intervention Proposal*. Department for Digital, Culture, Media, and Sports. https://www.gov.uk/government/consultations/app-security-and-privacy-interventions/app-security-and-privacy-interventions

United Kingdom Medicines & Healthcare Products Regulatory Agency, (2022). *Chapter 10: Software as a medical device*. UK Medicines & Healthcare Products Regulatory Agency. https://www.gov.uk/government/consultations/consultation-on-the-future-regulation-of-medical-devices-in-the-united-kingdom/chapter-10-software-as-a-medical-device

United Kingdom Department for Digital, Culture, Media, and Sports, (2022). *Product Security and Telecommunications Infrastructure Bill*. UK Parliament. https://bills.parliament.uk/bills/3069

Woodard, R. (2021). *Encryption and Export Administration Regulations (EAR)*. Bureau of Industry and Security: Department of Commerce. Retrieved August 24, 2022, from https://www.bis.doc.gov/index.php/policy-guidance/encryption

Zambian Ministry of Information and Communications Technology, (2021). *Cybersecurity and Cybercrimes Act*. Zambian Ministry of Information and Communication Technology.