Technological Collaboration in a Closing World

THE GUARDIAN PROJECT
https://guardianproject.info

PRUDENT INNOVATION
www.prudentinnovation.org

About The Guardian Project

While smartphones have been heralded as the coming of the next generation of communication and collaboration, they are a step backwards when it comes to personal security, anonymity and privacy.

Guardian Project creates easy to use secure apps, open-source software libraries, and customized mobile devices that can be used around the world by any person looking to protect their communications and personal data from unjust intrusion, interception and monitoring.

The Guardian Project's core application suite (Orbot, Orweb/Orfox, ChatSecure, FDroid, etc) provide a baseline set of privacy and security capabilities to the common activities of browsing, messaging and getting apps on an Android smartphone. They have shipped multiple releases over the past 4 years, utilizing best practices for free software projects, community driven development, and support for tested technologies and open standards, such as Tor, OTR, XMPP, and Firefox. In addition, they have acted as a catalyst to do the initial development work on ports to Android for technologies like SQLCipher, GnuPG, Tor, Privoxy, and even Debian.

About the Author

Seamus Tuohy is the principal consultant at Prudent Innovation LLC. Prudent Innovation provides technical and security guidance, development, research, and programmatic support to organizations working in complex or hostile environments. Mr. Tuohy has worked with donors, Human Rights defenders, Civil Society, and International NGOs around the globe to to assess, address, and adaptively manage risks in their work. He is also one of the chief architects of "The Security Auditing Framework and Evaluation Template for Advocacy Groups" (SAFETAG), which adapts traditional risk assessment methodologies to be relevant to low-resourced non-profit organizations based or operating in the developing world.

Executive Summary

Introduction

The Guardian Project has been working with the FDroid community to make it a secure, streamlined, and verifiable app distribution channel for high-risk environments. While doing this we have started to become more aware of the challenges and risks facing software developers who build software in closed and closing spaces around the world.

There are a wealth of resources available on how to support and collaborate with high-risk users. Surprisingly, we could not find any guidance on how to support and collaborate with developers where the internet is heavily monitored and/or filtered, let alone developers who might be at risk because of the software they develop.

This report explores some key challenges that developers in closed and closing spaces face when collaborating with international[1] groups who support Human Rights and freedom (IHRFG). These groups include privacy and security software projects, civil society focused donors, and non-governmental organizations (NGOs).

IHRFG can benefit greatly from collaborations with local developers. IHRFGs who are trying to design or localize software for a specific region often have difficulty

- understanding the types of technologies that are needed to address the problems IHRDGs are trying to solve,
- addressing the local economic, social, infrastructural, and/or legal challenges that software of its type often faces in the local context,
- identifying the interaction and design patterns that will drive initial adoption,
- evaluating the quality of the translations of software into the local language,
- finding local individuals for focus groups, and testing, and
- conducting testing and troubleshooting to identify and address issues caused by the speed, availability, and/or censoring of local fixed or mobile networks.

Local developers, on the other hand, are often more than able to accomplish these tasks.

Beyond identifying these challenges this report provides guidance on how to take these challenges into account when IHRFGs collaborate with local developers. It also contains a set of

[1] Both author of this paper and the Guardian Project are based in the United States of America. As such, while we conducted interviews with international Human Rights and freedom groups (IHRFGs) and developers from all over the world the community of IHRFGs that we are most familiar with are the western Human Rights and Internet Freedom communities. The guidance and user-personas will likely have unintended biases towards these communities.

developer user-personas. These personas can be used by IHRFGs as an aid when they are designing collaborating with local developers.

We hope that the results of this research will help international privacy and security focused software projects and NGOs better understand and respond to the unique needs of different international developer communities so that their collaborations with these developers will be safer, more strategic, and sustainable.

Research Methodology

This report is the result of two interconnected streams of research. The initial themes were identified in a series of in-depth interviews. These themes were further explored in an online "developer challenges survey." The challenges and user personas found in this report were refined from the combined results of these research efforts.

Interviews: interviews with 14 developers, technologists, and digital defenders from 11 different countries where the internet is heavily monitored and filtered as well as 5 interviews with IHRFGs who work in similar regions.

Surveys: an online developer survey in Chinese, Spanish, Farsi, Russian, French, and English that received 118 responses from developers in 28 countries around the world.

Local Context

The local context deeply impacts the needs, goals, and challenges of developers who are collaborating with international groups who support Human Rights and freedom (IHRFGs). The macro level characteristics of a country create an environment that local development communities must operate within. The ways that each developer responds to their environments depends upon on a variety of other factors. By understanding what these characteristics are, how they change the environment that a local developer operates in, and how it impacts a developer's ability to collaboration with an IHRFG an IHRFGs can make more informed decisions about how they engage in collaboration.

In this section we discuss country level characteristics that can impact a developer's ability to collaborate with IHRFGs. This report divides these key country-level characteristics into four categories: Economic Characteristics, Infrastructural Characteristics, Collaboration Laws, and the Rule of Law.

Economic Characteristics

The impact of state level economic policies and sanctions should not be underestimated when looking to understand a developer's interest and ability to collaborate with outside actors. Both the level of economic isolation and economic disparity of a state have clear impacts on a local developers ability to engage in international commercial and collaborative spaces.

If a state is economically isolated a developer will be unable to engage in financial transactions with possible collaborators. The general economic disparity that exists between a local developer, international technological markets, and possible collaborators impacts the developers ability to engage outside of their country.

Economic Isolation

The level to which a developer can engage in global financial systems impacts their willingness to work with International actors. Both internationally imposed sanctions and internally imposed economic isolation impedes a developer's ability to engage in financial transactions with online services and possible collaborators.

Economically sanctioned states have externally imposed restrictions that economically isolate developers. Examples[2] include the United States sanctions against Iran[3] and the international economic sanctions against Crimea[4,5].

There are two specific aspects of economic sanctioning that directly impact local developer communities.

1. These sanctions often forbid the sale, supply, transfer, or export of technology to a country. This forbids international online services and/or software retailers from selling services and software licenses to local developers. In the Iranian case there have been "Internet Freedom" exceptions made for personal communications software.[6,7] And, while these exceptions allow web-hosting and online advertising programs to apply for "specific licenses" on a case-by-case basis, these exceptions do not vastly improve local developers access to the range of cloud based services that support software planning, development, testing, release, or management.
2. The investment and trade embargoes that come with sanctioning make it nearly impossible for collaborators to pay developers in an economically sanctioned state. Even in the best case, when IHRFGs have a general license[8][9] to collaborate with local developers, collaborators face significant challenges transferring funds to local developers they are collaborating with.

Economically isolated states have locally imposed foreign exchange and/or currency controls that create significant barriers for local developers to engage in business internationally. These controls are implemented for a variety of macro-economic reasons.[10] Foreign exchange controls are imposed by a country to "restrict monetary transfers through the regulation of:

---

[2] This section uses US sanctions for its examples because they are the most familiar to the author. The author does not have a legal background and the below interpretations of different sanctions should not be read as legal opinions.

[3] Iran Sanctions - https://www.treasury.gov/resource-center/sanctions/Programs/Pages/iran.aspx

[4] Ukraine-/Russia-related Sanctions - https://www.treasury.gov/resource-center/sanctions/Programs/Pages/ukraine.aspx

[5] International sanctions during the Ukrainian crisis - https://en.wikipedia.org/wiki/International_sanctions_during_the_Ukrainian_crisis

[6] INTERPRETIVE GUIDANCE AND STATEMENT OF LICENSING POLICY ON INTERNET FREEDOM IN IRAN

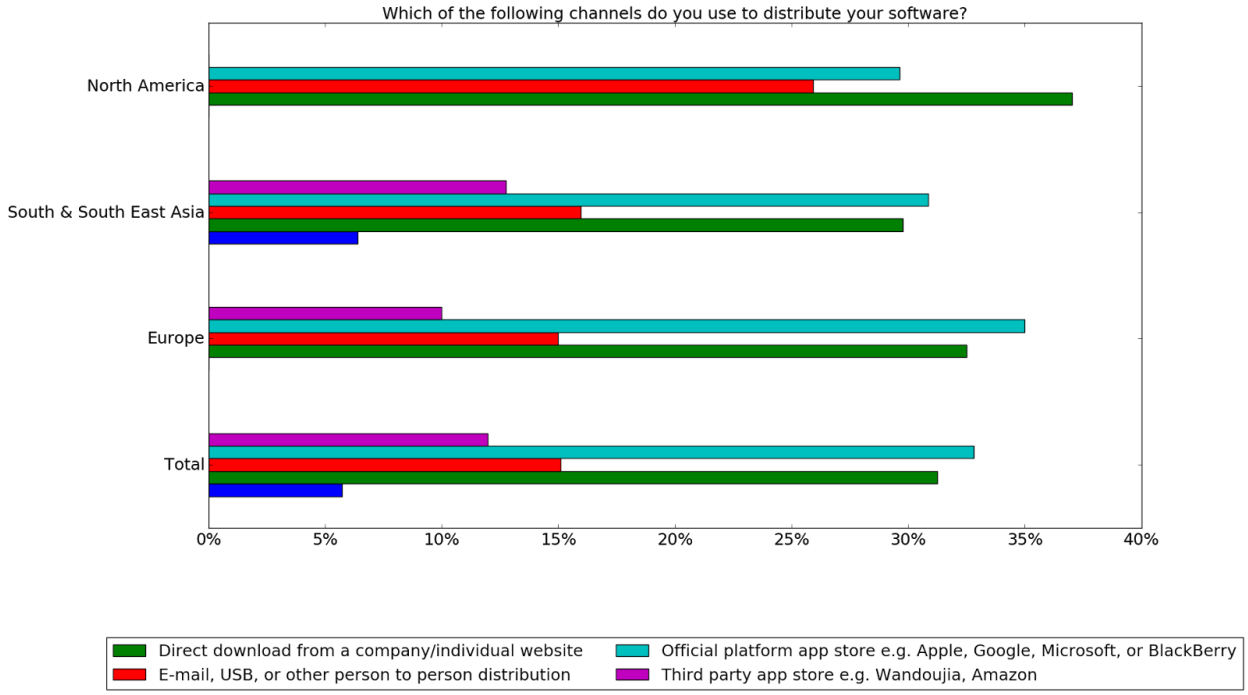
[7] Exportation of Certain Services and Software Incident to Internet-Based Communications Authorized
- https://www.treasury.gov/resource-center/sanctions/Programs/Documents/ukraine_gl_9.pdf

[8] Who is authorized to send money to support certain nongovernmental organizations' activities? - https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_other.aspx#205

[9] SYRIA GENERAL LICENSE NO. IIA - https://www.treasury.gov/resource-center/sanctions/Programs/Documents/syriagl11a.pdf

[10] There are far too many reasons to cover within this paper. Foreign Exchange Control: Definition, Objectives, Types and Conditions - http://www.economicsdiscussion.net/foreign-exchange/foreign-exchange-control-definition-objectives-types-and-conditions/13973

- currency convertibility, limiting the extent to which local currency can be converted into foreign currency;
- conversion rate, controlling the rate that can be obtained for such a transaction;
- the types of currencies with which payments may be made; [and]
- transferability of a currency off-shore and repatriation of profits off-shore."[11]



For local developers, these restrictions can make the exchange of international services and paid international collaboration very difficult.

1. Developers can face significant challenges converting their local currency into foreign currency. This makes it very difficult to purchase international online services and/or licenses for software produced internationally. Paid collaboration with IHRFGs can actually benefit local developers in this case as international collaborators may be able to support the local developers operations by allowing them to act as proxies using the foreign currency the local developer has generated abroad to pay for these international services.

[11] Restrictions on Foreign Investors/ Currency Exchange Controls - Public Private Partnership in Infrastructure Resource Center - http://ppp.worldbank.org/public-private-partnership/legislation-regulation/framework-assessment/legal-environment/foreign-investor-currency-exchange-restrictions

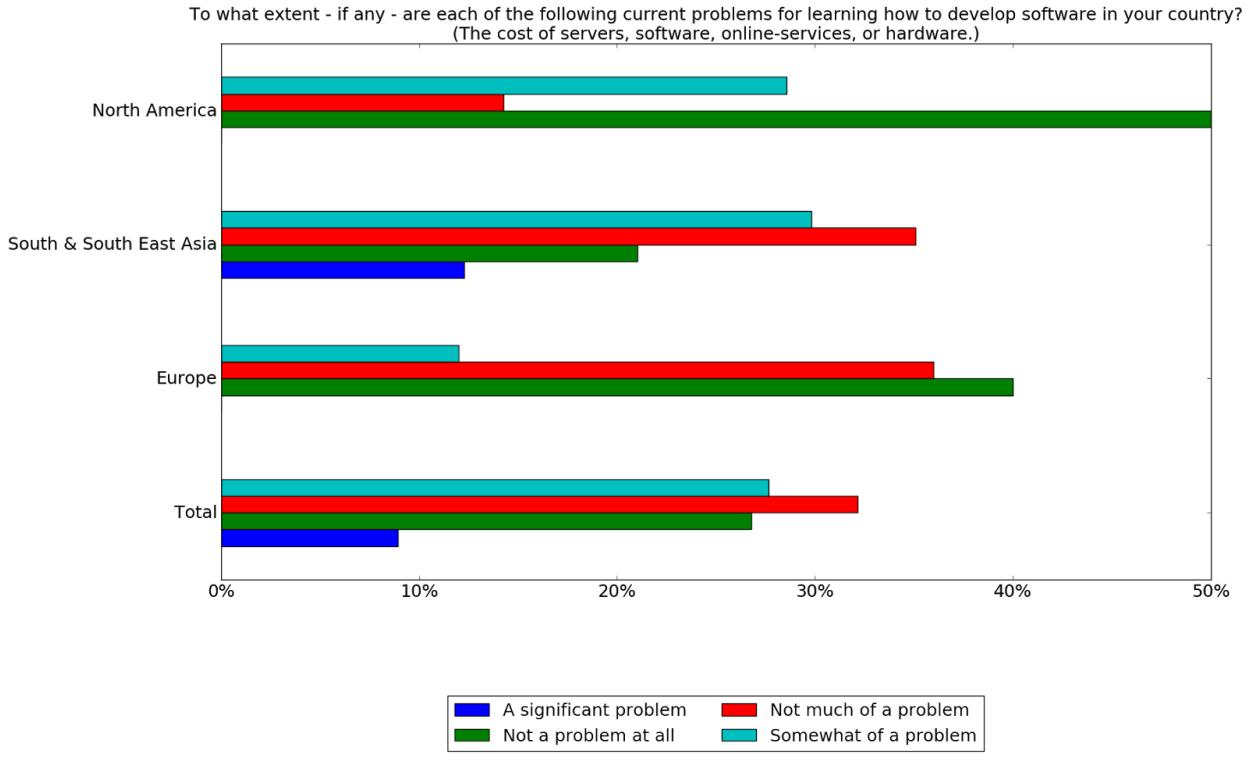
2. The inverse difficulty converting international currency into local currency can make it difficult for developers to benefit from online transactions (such as selling software in app stores) because they cannot convert their profits into the local currency.
3. IHRFGs often face complex hurdles when attempting to pay local developers in countries with foreign exchange and/or currency controls.
    a. These controls are often found in unstable economic environments and are often accompanied by high levels of inflation.
    b. The cost of labor is often divorced from the cost of living. When IHRFGs tie the wages of a local developer to an unstable inflation rate it can cause the underpayment or overpayment of local developers.
    c. Many countries with high and unstable inflation rates are lacking reliable ways of reporting the exact rate. This can lead to IHRFG finance departments having to reverse or increase payment after the fact. The friction this causes can spoil even long-term collaborations.

Economic Disparity

Challenges can also arise if there is significant economic disparity between local developers and the target user base of the international technology sector or between local developer and the IHRFGs they are collaborating with.

Many of the commercial software packages and cloud services used by developers around the world are sold using a single set of prices that are determined by their target markets. For example, developers in the United States will often price their products to United States customers and UK developers to those in the UK. They do this primarily because country specific pricing for a service comes with a range of additional hassles that make it unappealing: Determining the prices for specific regions; Protecting against fraud; and being responsive with exchange rate fluctuations are only a few of these challenges.

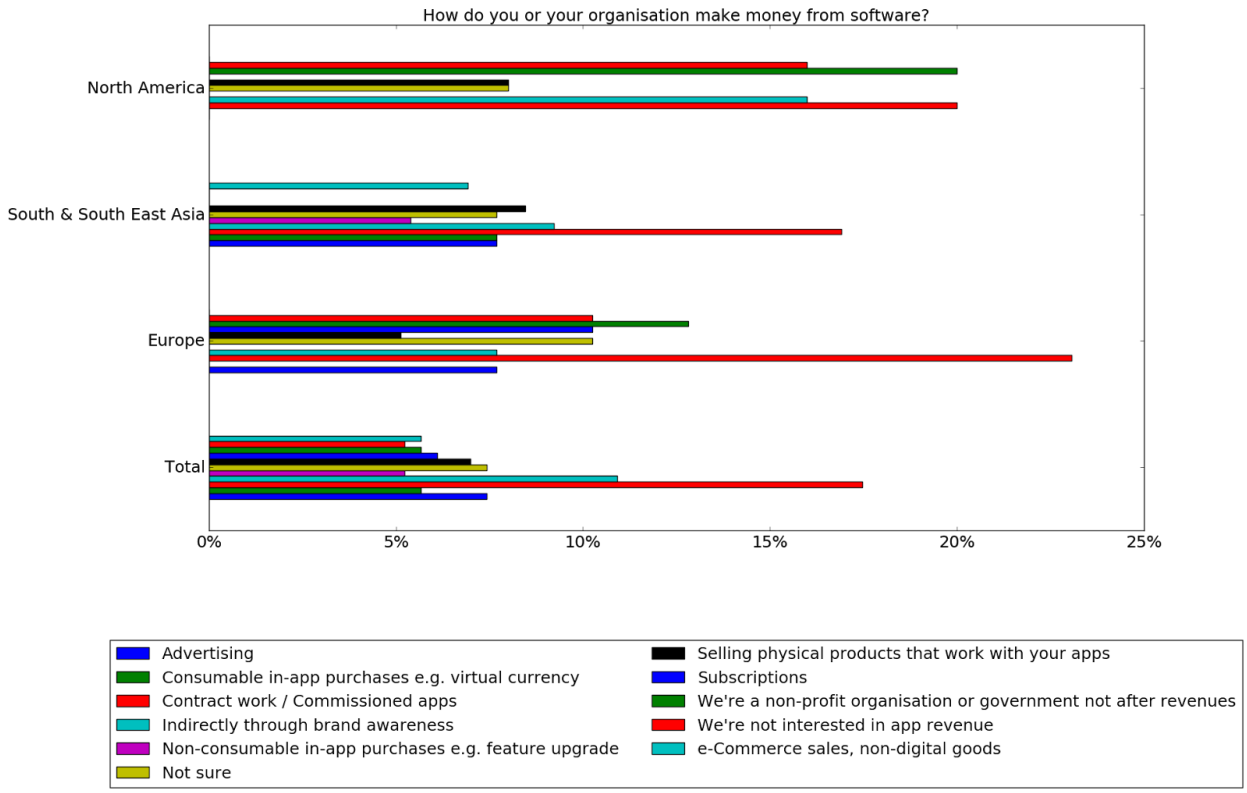
These single-market targeted price-points mean that a developer who has a lower income than developers in the services targeted country faces much higher costs relative to their income.



Software & Secondary Markets

When software price impacts a local developer's ability to legitimately purchase *desktop software* they often turn to local secondary (black) markets. These black markets give developers access to illegitimate copies of the development and design software they need to do their job effectively. The reliance on these secondary markets also adds an additional security challenge for local developers. The copies of software that are downloaded or purchased are often bundled with malware that can infect a developers machine.

Ironically, the use of these secondary markets by local users also means that developers have to protect their software from ending up in these secondary markets in order to impact their own ability to make a living developing software. This often occurs when local developers when pricing their products for western markets prices them to out of the range of local markets.



Local developers use a variety of tactics to combat this. They sometimes advertise local discount codes that make the price more reasonable for local markets. Some local secondary markets also are willing to support local local developers by removing software that is created locally.

Cloud Services

Cloud services are used by developers to support the planning, development, testing, release, and/or management of software and online services. These can streamline the development process by helping developers to get their own software and services up and running quickly, make these services more robust and less prone to going down, and allow them to be seamlessly scaled as their user-base grows.

Unlike software, cloud services cannot be “cracked” and redistributed on local markets. Without the financial resources to purchase these cloud services local developers have to do without. This forces them to make architectural decisions based on scarce resources and not based on how to provide the best services, security, and availability to their customers.

Collaboration

Everyone has to make decisions based upon their own financial realities. This is as true for IHRFGs as it is for local developers. These economic realities can add complexities to collaboration between IHRFGs and local developers.

The economic disparity between a local developer from a low and/or lower-middle income country and an IHRFG from a high-income country it creates a financial power imbalance. Research and best practices from the development and aid sector show that these imbalances are, to an extent manageable.

These imbalances open up a range of unique risks for technological collaborations around Human Rights and freedom issues. When developers lack expertise working with at-risk or vulnerable populations they are at risk of being in a position where they can develop and legitimize a product or service which could potentially have harmful impacts for their local community. Furthermore, Human Rights and freedom work has a range of risks associated with it. But, a local developer must weigh these risks against their own financial needs. When income is scarce, or payment is unusually high, a local developer may be willing to take a greater level of risk than they would otherwise be comfortable with.

IHRFGs can make strides towards addressing the impacts of financial power imbalance by actively engaging local developers in a collaborative evaluation of the risks associated with the project being conducted, modification of the project's activities to make them safer, and/or the design of more appropriate alternative activities. Ensuring that the mitigation put in place are grounded in a shared understanding of the acceptable risks of all parties helps ensure that these collaborations do not force local developers to choose between their financial needs, ethical principles, and personal security.

As skilled labor local developers in low and/or lower-middle income countries may have to make decisions that compete with IHRFGs goals because of their local financial situation. One example of how this can manifest comes from the international aid and development space. Development projects that aim to build local skilled labor capacity often provided training and/or other skill-development to local actors. Some of those actors, in turn, leverage those new skill in their attempts to migrate out of their country. These local actors have to make the hard decision between the stated long-term regional benefits of an aid organization’s project if the local actor stays and migration which can have financial benefits for their families, communities, and self in a variety of ways.[12]

IHRFGs should be mindful how economic disparity can impact decisions local actors make when designing collaborations. The financial power Imbalance that comes paid collaboration can have. This can cause a range of unintentional effects if it is not addressed. It can push a

[12] For a more in-depth exploration of these effects see: Skilled migration: the perspective of developing countries

local developer to silently take a greater level of risk than they would otherwise be comfortable with. Projects also can suffer from these imbalances as they remove many of the benefits of collaboration with a local developers. For instance, it can stifle their willingness to disagree with IHRFG recommendations and requirements that may be detrimental to the project. Addressing this can be done, to a large extent, by ensuring that collaborations with local developers are truly collaborations where each party is an active partner in the initiatives who has a say in the design and implementation of the project.

Local Infrastructure Characteristics

A developer's local technical infrastructure impacts their needs, goals, and challenges. This infrastructure includes both local communications infrastructure used by a populace to connect to the internet, as well as local cloud computing infrastructure that a developer use to support their work.

Local Physical Communications Infrastructure

Local communications infrastructure impacts the ability of developers and their local users to access online services and information. The level of availability, connectivity, and censorship each have unique repercussions. These repercussions are wide ranging. We will only explore some key developer centric impacts that are relevant for the purposes of this paper.

Low Availability

Availability is the overall level of access a population has to the internet. When there is limited availability in a region it is often the result of limited communications infrastructure, the result of limited electric infrastructure where brown/black-outs cause that infrastructure to be rendered useless, or wide-scale or targeted censorship.

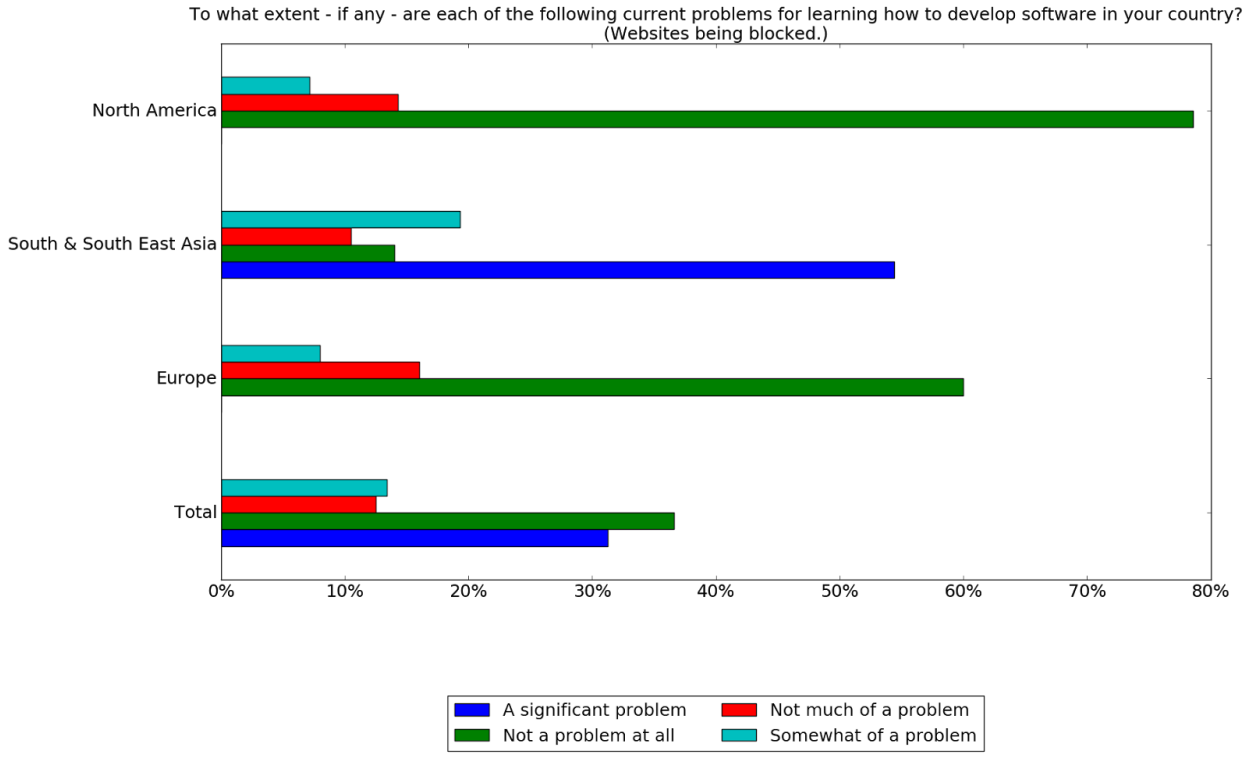
Lacking or inconsistent access to the internet changes the way a developer will make decisions about how they build software and services. A developer who hosts an online service in their home, or garage, will have a service that is as consistent as the infrastructure they are provided. This removes the option of self hosting in areas with low availability. The archetypal Silicon Valley “garage startup” cannot happen in an area with inconsistent access.

Local developers understand how low access and intermittent connectivity impact their local users. Low availability means that software has to be designed to work offline so that it can handle unreliable connectivity. Local developers, as consumers themselves, understand and make strategic design decisions for services they are developing for their local markets. Some of these core principles for developing services and software for the needs of low-availability markets have been documented.[13] Developing software for a local market with low availability requires a deeper understanding of how that specific user base addresses these challenges. A

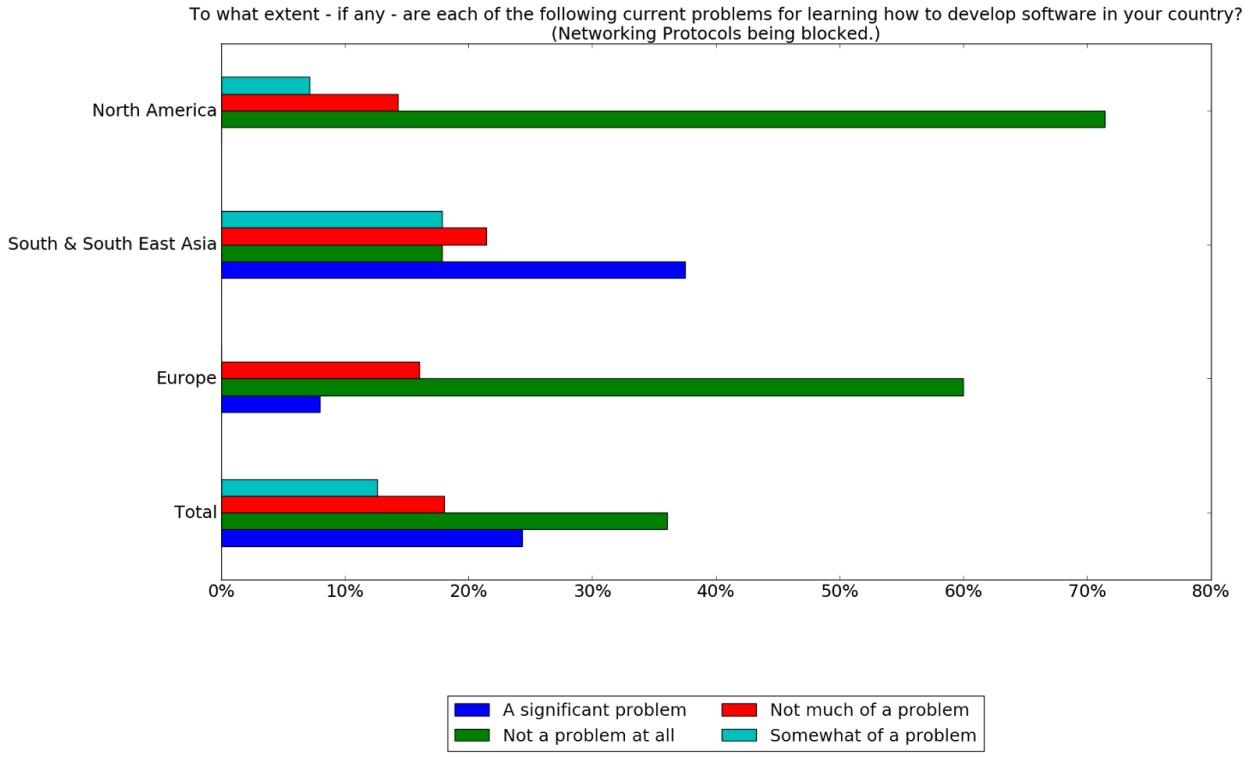
[13] Building For Billions - https://developers.google.com/billions/

local developer's understanding of how local technical context impacts the adoption of services and software is one of the reasons why collaboration with local developers is so critical for IHRFGs.

Free access to computers, sharing, and openness are core tenets of the "hacker ethic,"[14] a seminal set of principles for software development communities around the world. As we discuss further in the "Developers Worldwide" section of this report, access to online educational resources and technical communities is a highly valuable resource for individuals educating themselves in software development. Widescale and targeted censorship has specific challenges for those learning software development. When technology students are unable to freely seek out learning resources, use social media to get advice and guidance, or experiment with different technologies they are put at a disadvantage.



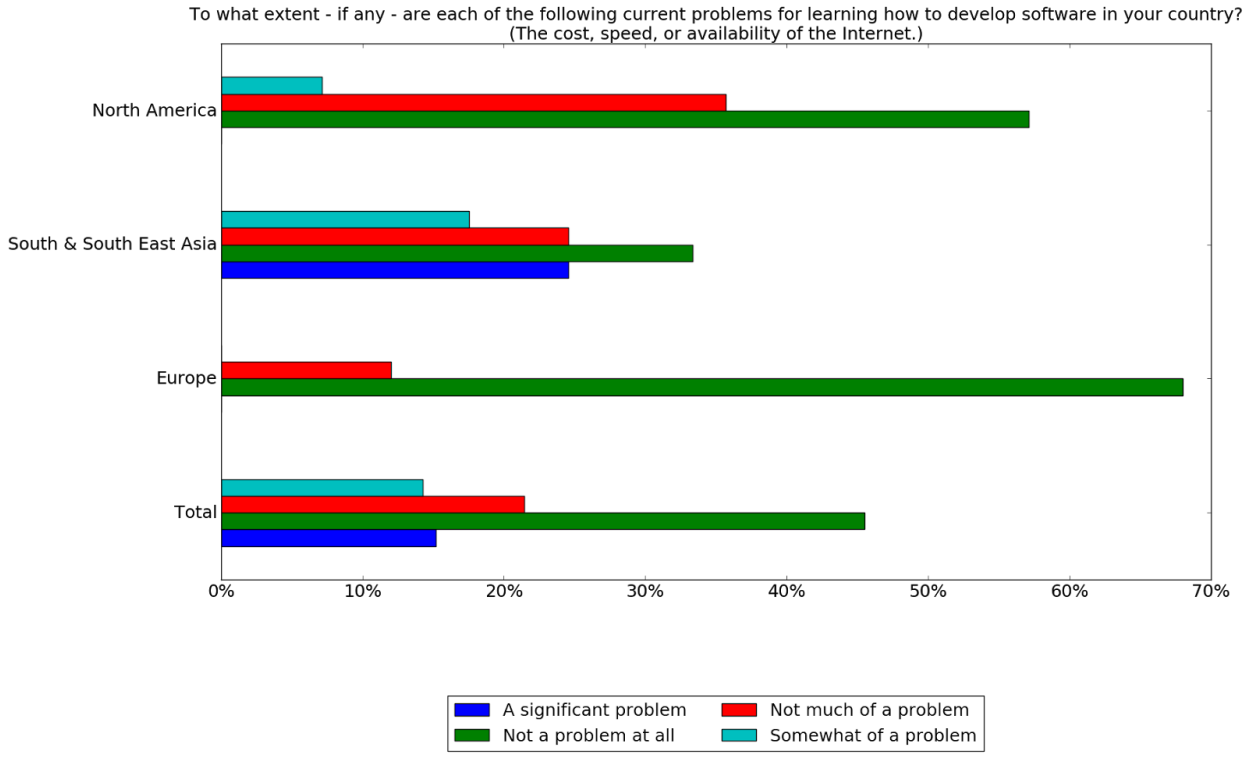
[14] https://en.wikipedia.org/wiki/Hacker_ethic



Limited connectivity

For the purposes of this report, connectivity includes barriers to data usage on a local networks. This includes both the speed of the network as well as the cost of using it to transfer data. Limited connectivity often is the result of insufficient infrastructure being used for the local population, communications infrastructure being too costly for them to use it freely, and/or the strategic use of throttling to inhibit free speech (censorship).

Limited connectivity impacts the development environment within a country. Similarly to limited availability, limited connectivity increases the difficulty of learning how to become a developer. Students are unable to freely seek out learning resources due to the cost or speed of the internet.



Once a developer has has gained the basic skills they need limited connectivity also increases the difficulty of developing software. When seeking out, finding, downloading, and testing alternatives is both slow and costly and other local developers are able to provide the libraries, software, and documentation they use via offline means development monocultures can form around specific software libraries and tools.

> "One interesting possible side effect of these overly onerous processes for accessing outside content [for North Korean software developers] is the large amount of code reuse found within Red Star OS and in North Korean-attributed malware. This begins to make far more sense when one considers that the process to search online for the appropriate documentation or example code can take upwards of a month. Reusing existing working codes from other projects would be far easier than seeking out solutions on the global internet." - Compromising Connectivity[15]

[15] Compromising Connectivity - http://www.intermedia.org/wp-content/uploads/2017/02/Compromising-Connectivity-Final-Report_Soft-Copy.pdf#page=62

Even as the access to the internet is increasing around the world[16] the cost of accessing the internet can be significant.[17] The bloat that advertising brings to websites further exacerbates this problem.[18] Developers who are building websites for users in areas of limited connectivity have to balance the attractiveness, performance, and profitability of their web-services during the design phase.

Infrastructural impacts

Much like economic disparity, low availability and low connectivity encourage the local sharing of software libraries, applications, and content in a region. The infrastructural barriers change the way that sharing is done. Offline means of sharing, such as sneakernets[19] and peer-to-peer bluetooth media sharing[20,21,22], become far more prevalent in areas with severely limited infrastructure. When an existing developer community also exists it is not unusual to find local area[23] and community wireless networks[24, 25] that are built to allow local connectivity and services, even if they don't connect to the wider internet. For example, the Athens Wireless Mesh Network (AWMS) offers communication services (VoIP telephony, fora, mail servers, instant messaging applications), data exchange services (P2P file sharing, FTP servers, video / image / audio galleries), entertainment services (online multiplayer games, audio and video streaming), as well as information and education services (online tutorials, wikis, weather forecasting).[26]

Infrastructure is a critical consideration when IHRFGs are deciding whether to seek collaboration with local developers. It is important to develop software and services that are responsive to the software and service requirements created by the level of availability and connectivity of local infrastructure. Local developers are uniquely positioned to build software that responds to their local infrastructural context because of their lived experience. IHRFGs should work collaboratively with local developers to develop software requirements that are responsive to the state of the local infrastructure.

---

[16] Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies - http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-climb-in-emerging-economies/
[17] What does my site cost - Cost as a percentage of GNI (PPP method) - https://whatdoesmysitecost.com/#gniCost
[18] Website Loading Slowly? You Can Probably Blame Ads
[19] Cuba's homemade Internet, delivered by sneakernet
[20] YouTube Go App Coming with Offline Viewing, Bluetooth Sharing with Friends
[21] TECHNOLOGY USE AND NON-USE BY LOW-INCOME BLIND PEOPLE IN INDIA
[22] Where There's a Will There's a Way: Mobile Media Sharing in Urban India
[23] Tech-Savvy Cubans Build Their Own Private Internet
[24] List of wireless community networks by region
[25] Second Summit on Community Networks in Africa
[26] AWMN FAQ - Συχνές Ερωτήσεις - Απαντήσεις για το AWMN

Local Cloud infrastructure

Cloud services are used by developers to support the planning, development, testing, release, and/or management of software and online services. Cloud services, such as those discussed in the earlier section on economic considerations, are not the only cloud services available to developers. Local cloud infrastructure are cloud services that are hosted within a developer's own country. Developer reliance on local Cloud infrastructure is becoming more widespread as technological, network, and data sovereignty laws around the world are forcing developers to use host and process data within their own country.

Technological, network, and data sovereignty laws are efforts for a government to exert control over digital activities that occur within the borders of their state. These laws are used by countries around the world to protect their citizens from being spied upon by foreign governments, ensure that their security forces are able to access their own citizens data, control the information their citizens have access to, and support the development of their local technology industry.

These laws are increasingly requiring that hosting and/or processing of its citizens data be done within their own country. For example, "the storage of [Kazakhs] personal data is only allowed through databases located in Kazakhstan;"[27] Russian citizen personal data must be collected, actualized, and stored in databases stored in Russia,[28] and in a draft cybersecurity in China "operators of key information infrastructure must store important data, such as personal information, within the territory of China."[29] These laws *tether the cloud* forcing developers who are building services for local audiences to use local services. Mandating use of local clouds can have a range of short and long-term impacts.

When mandatory usage of local cloud services is combined with more widespread limited availability and/or connectivity in the region local developers are forced on to less reliable local infrastructure instead of more consistent international services. This is compounded in areas with newly developing technology sectors. In these environments technology and data sovereignty laws push an entire population of developers into a local technology sector whose services are often lagging behind industry standards.

Even in well-developed technology sectors technological consumer rights regulations are straining to keep up with technological advances. In developing tech sectors consumer protection laws are often far behind, or completely missing. Local developers who are required to use local cloud services can face a tech sector comprised of service provider monopolies that have little interest, or legal obligation, to push themselves to compete with their previous global competitors.

[27] https://iclg.com/practice-areas/data-protection/data-protection-2016/kazakhstan#content-c11
[28] https://iclg.com/practice-areas/data-protection/data-protection-2016/russia#chaptercontent11
[29] https://iclg.com/practice-areas/data-protection/data-protection-2016/china#chaptercontent8

Tech sovereignty does offer opportunities for local developers as well. Mandatory local usage in developing regions creates unique opportunities for local developers to build out services in local cloud service markets without having to compete with western cloud-giants (google, amazon, etc.).

Local cloud infrastructure and technology and data sovereignty laws are critical considerations when IHRFGs are deciding whether to seek collaboration with local developers. There are a variety of reasons why these projects might wish to not host data in cloud services within a country, such as when IHRFGs are working with populations that are targeted by the local government, or when the services that are being created are likely to be censored. When considering collaboration with local developers IHRFGs should consider the difference in the risks profile associated with the improper use of international hosting and/or cloud services when they are implemented by an IHRFG as opposed to when they are implemented by a local actor.

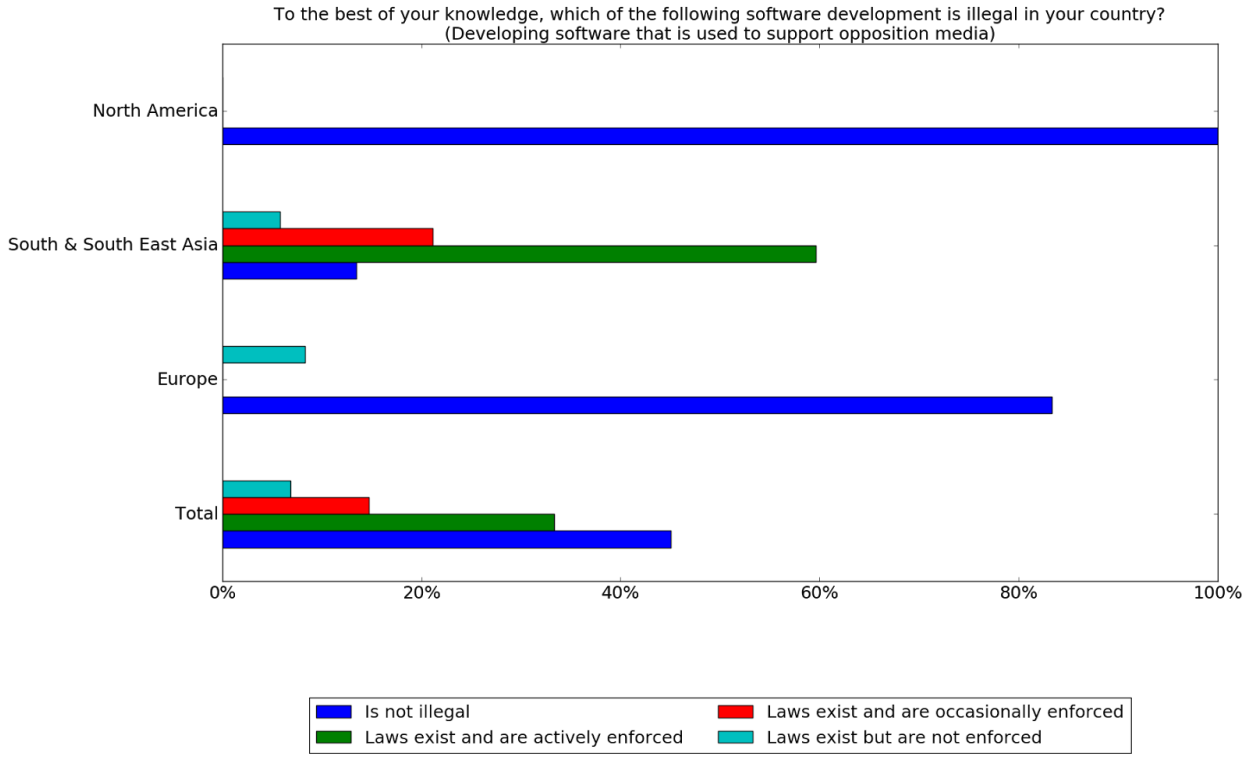
Collaboration Laws

Collaborating across state boundaries means collaborating within different legal codes, and in environments with different levels of the rule of law. Governments around the globe have become increasingly more subtle in the ways that restrict the environment that civil society can operate within. In many closed and closing spaces legal, or quasi-legal barriers, have been put in place to frustrate the activities of civil society. Among these are barriers that restrict the ability of local developers to conduct specific types of civil society focused development activities and to engage with IHRFGs.[30]

One of the chief ways that collaboration between IHRFGs and local actors are frustrated are through laws that restrict whom local actors are able to receive funding from. A majority of these laws around the world are targeted specifically at local non-governmental organizations seeking funding from international donors.[31] The civil-society focused nature of some of these laws can allow paid collaborations between IHRFGs and developers who operate as for-profit entities to avoid these restrictions. But, this is not always the case. In Egypt, for example, no association may receive foreign funding without prior approval from the Minister of Social Solidarity and Justice.[32]

[30] There are far more legal barriers put in place to frustrate local civil society than just barriers to collaboration and activities. For the purposes of this paper we will only explore legal complexities related to collaborations between local developers and international collaborators that might pose a risk to a local actor. We will also not be exploring the complexities of international legal contracts, including which countries laws may apply to contracts, or how copyrights, patents, and/or liability applies and is enforced.
[31] http://fatfplatform.org/foreign-funding-restrictions/
[32]Defending Civil Society Report - http://fatfplatform.org/wp-content/uploads/2015/02/DCS_Report_Second_Edition_English.pdf#page=28

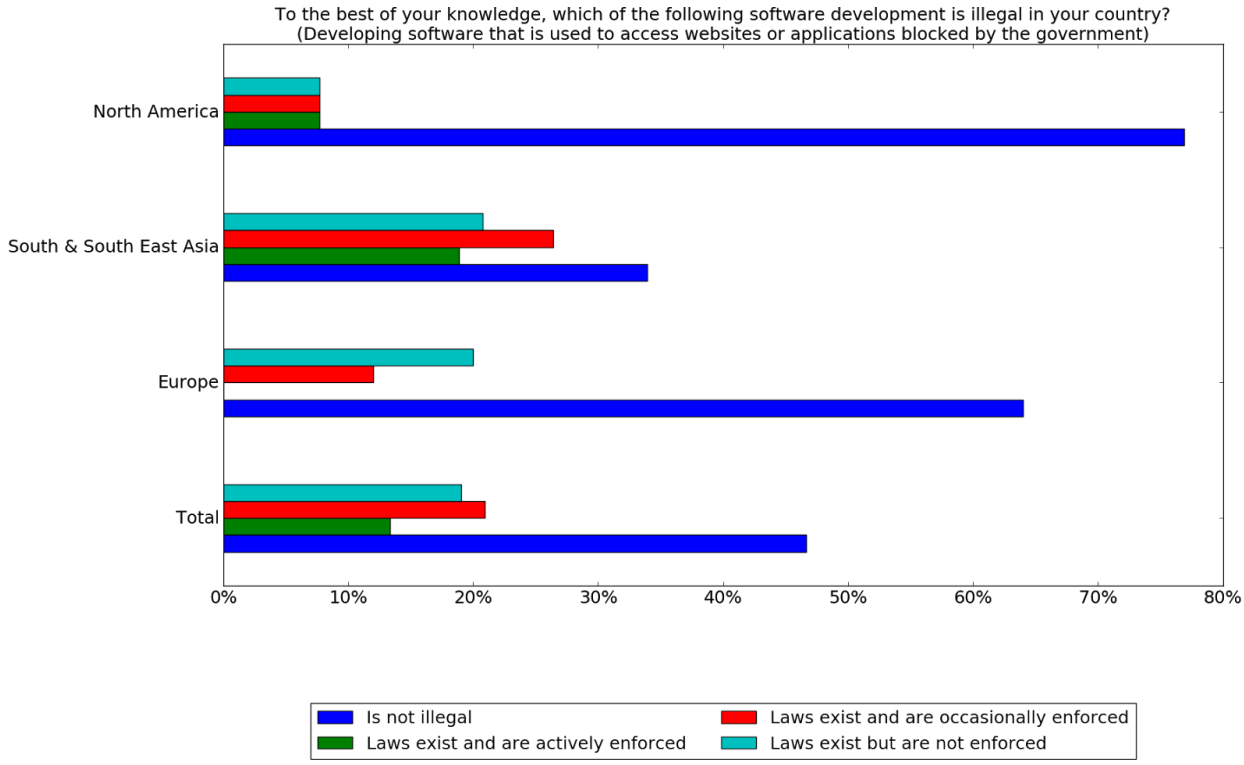
In some cases, it is the nature of the work that determines whether or not the funding is allowed. Often the vaguely worded nature of the laws allows these laws to be used as needed by a government to quell civil society activity. An example of this is in India where foreign funding not allowed for “Organization[s] of a political nature.”[33] What makes an organization qualify as being “of a political nature” was not defined. In other cases, such as in Indonesia, the restrictions are far clearer. “In Indonesia, the 2008 regulation on the Receipt and Giving of Social Organization Aids from and to Foreign Parties prohibits foreign assistance causing “social anxiety and disorder of national and regional economy.”[34]



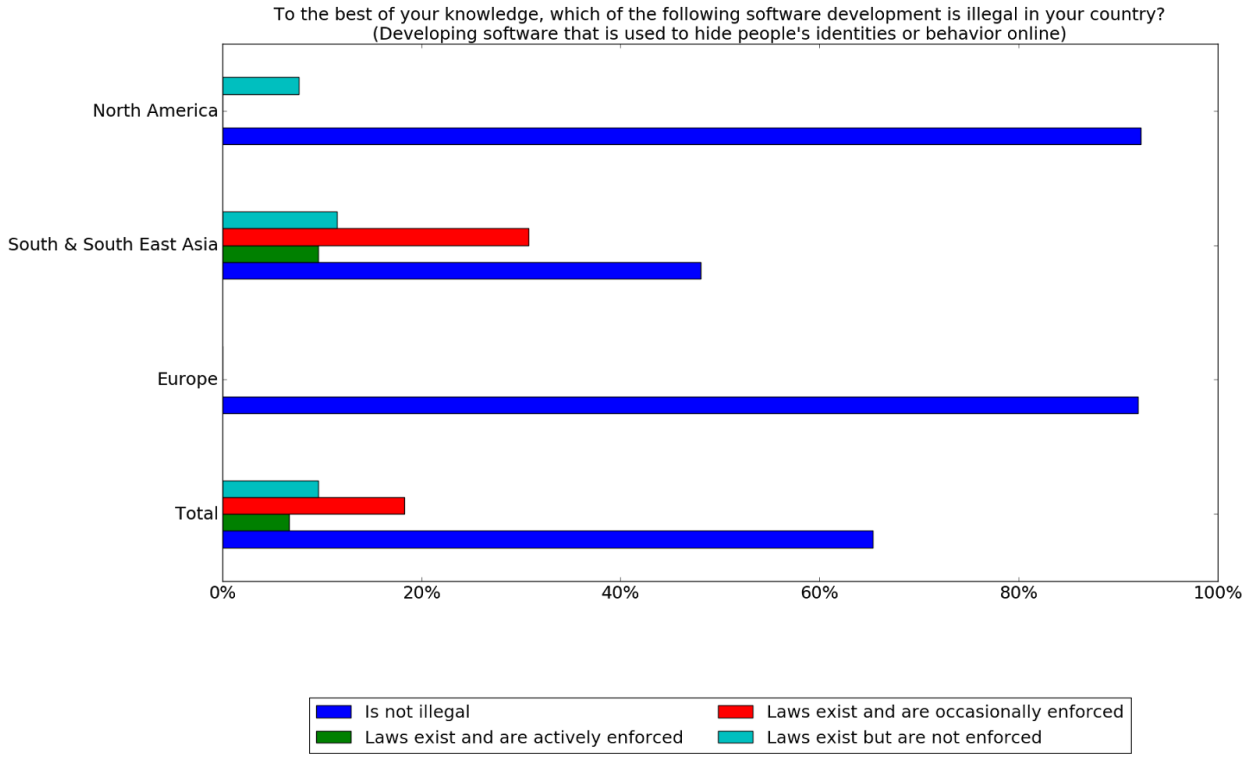
Laws that specificly target more widely know or effective IHRFGs have also started to appear. These laws make it far easier for local developers to be sanctioned if they collaborate with specifically identified IHRFGs. Russia's “undesirable organizations” law is the most prominent example of this. Under this law any foreign or international NGO that the Russian government declares as “undesirable” will be banned from working in Russia. And, in addition, any individual or organization that collaborates with them on activities inside the country faces penalties.

[33]Defending Civil Society Report - http://fatfplatform.org/wp-content/uploads/2015/02/DCS_Report_Second_Edition_English.pdf#page=28
[34]Defending Civil Society Report - http://fatfplatform.org/wp-content/uploads/2015/02/DCS_Report_Second_Edition_English.pdf#page=29

"Anyone working for an "undesirable" organization—including in an unofficial capacity—faces fines of up to 15,000 rubles (about $300) for ordinary citizens, up to 50,000 rubles ($1,000) for officials, and up to 100,000 rubles ($2,000) for the organization itself. Criminal proceedings will be initiated against repeat offenders and the punishments can be even harsher, with fines of up to 500,000 rubles ($10,000) and prison sentences ranging from two and six years." - Meduza[35]



[35] https://meduza.io/en/feature/2015/05/19/the-most-draconian-law-yet



Making the decision to respect local laws or not is a difficult decision that IHRFGs have to make.[36] When an IHRFG makes the decision to ignore, or skirt, local laws it is important that they share these decisions and the possible risks involved with local developer collaborators. Local developers, especially those who do not often work in the IHRFG space, may not be familiar with local laws that surround international collaboration. “Plausible deniability” is neither ethically nor legally useful in environments where this type of collaboration is sanctionable.

As “unregistered entities” collaboration with local for-profit developers may be a way to include local collaborators in your projects when funding local civil-society is illegal. But, as many of those we interviewed noted, and will be discussed in more depth in the next section, in many countries around the world the laws are vague enough to allow government agents to find one way or another to sanction an individual or organization. In these cases clever legal loopholes may only protect the IHRFG.

Rule of Law

IHRFGs must account for the local rule of law when exploring possible collaborations with local developers. In areas where the rule of law is weak what makes one applicable for sanctioning

[36] Closing Space: Democracy and Human Rights Support Under Fire - http://carnegieendowment.org/files/closing_space.pdf#page=62

and the severity of that sanctioning can seem arbitrarily decided. The local actors who make these decisions can be just as varied. In some areas non-state actors are as much, if not more, responsible for sanctioning local actors than individual government officials. Local developers may not know what activities will cause them to be targeted, what laws, if any, will be used to target them, and how severe the penalties will be.

Applicability for sanctioning

Local developers who are collaborating with IHRFGs often have to worry about being targeted for conducting both illegal technical activities and/or "harmful" development activities. Illegal technical activities refers to technical activities (development, IT support, etc) that are in themself illegal (ie. conducting computer or network sabotage through viruses, worms, Trojan horses, denial-of-service attacks) or that are used to aid and abet illegal activities. Harmful technical activities, on the other hand, refer to technical activities that, without illegality, are deemed to be against good morals or other social orders.

When developers collaborate with IHRFGs one of the challenges they face when translating project activities to the local context is the differences in legal codes. Activities that are legal, or unenforced, in one country can be illegal in another. IHRFGs often lack the capacity to do in-depth legal assessments in all the areas they wish to work, and local developers often only have a cursory understanding of the legal environment surrounding Human Rights and Freedom work within their region or the level of risk they are taking by participating in that work. What technical activities makes one applicable for sanctioning in closed and closing spaces can be difficult to determine if that individual is not a local legal professional who specializes in this area.

In many closed and closing spaces individual government officials are able to arbitrarily target specific actors for sanctioning. One side effect of arbitrary targeting is that in many cases it is the public facing members of a local Human Rights or Freedom project who are targeted, not the individuals, like developers, who support these activities.

While, historically, technologists have been mostly free from targeting because of their background role, as IHRFGs increasingly engage in the technological arena governments are starting to look to local developers who "aid" those activities as "proxies" for sanctioning that cannot be levied directly against the IHRFG.

Recently, technologists around the world have started to face sanctioning for "harmful" technical activities that, while not illegal, are deemed to be against good morals or other social orders. Saeed Malekpour, is a Canadian developer who was arrested in 2008 during a short trip to visit his father in Iran. Malekpour was targeted by the Iranian government because,

unbeknown to him, others had used open source code he developed to upload pornographic images to the Internet.[37]

> "Malekpour was told his name had been found on software being used on pornography sites. They accused him of managing obscene websites. His later charges included "spreading propaganda against the regime," "insulting Iran's supreme leader and president," "contact with foreigners and opposition groups," and "blasphemy." Malekpour was tortured until he confessed to these crimes, and more." - Electronic Frontier Foundation[38]

This type of "proxy targeting" of local developers is a dangerous precedent that highlights the difficulty local developers face in identifying and making strategic decisions about the risks they will take.

This seemingly inconsistent targeting does not just apply to those who are directly engage in the activities deemed to be illegal or harmful. There are times when, for political, public image, or other reasons government agents decide it is unwise to sanction an individual or organization for their activities. In areas with limited rule of law security forces have been known to turn to harassing, sanctioning, or even kidnapping a targets loved ones.[39,40]

Collaboration between IHRFGs and local developers should address how the differences in laws, and how they are enforced, impact how to safely collaborate. This will impact which activities each party should be in charge of. These collaborations must find an acceptable legal ground in each applicable local for each parties individual activities to take place. Finally they should explore how anonymity and pseudo anonymity might be used to conceal the identity of the IHRFGs, the local developer, or their relationship in order to reduce the likelihood of a local developer being targeted.

Severity of sanctioning

In areas with limited rule of law, the severity of the sanctioning that a targeted local developer faces is often as inconsistent as what made them applicable for targeting.

Developers, above other local actors, also face increased sanctioning because their work occurs within the digital realm. In most countries around the world the definition of a "cyber crime"

---

[37] Help End the Imprisonment of Iranian Web Developer Saeed Malekpour- https://advox.globalvoices.org/2016/10/03/help-end-the-imprisonment-of-iranian-web-developer-saeed-malekpour/

[38] Offline: Saeed Malekpour - https://www.eff.org/offline/saeed-malekpour

[39] Treatment by Iranian authorities of relatives of persons who have left Iran and claimed refugee status, including former members of the Bureau of National Security and Intelligence (SAVAK), of a Fedayeen organization, or opposition protestors [IRN103327.E] - http://www.ecoi.net/local_link/132597/244832_de.html

[40] Unmatched Power, Unmet Principles: The Human Rights Dimensions of US Training of Foreign Military and Police Forces - https://www.amnestyusa.org/pdfs/msp.pdf#page=10

makes it so the sanctioning for any illegal or "harmful" activity that is conducted using technology is significantly increased. For example, it is illegal to use a VPNs and other circumvention technology in the United Arab Emirates to commit a crime or prevent the discovery of a crime. The punishment for using a VPN in this way are fines between Dh500,000 (136,124 USD) and Dh2 million (544,499 USD) as well as temporary imprisonment.[41] These sanctions are in additional to the sanctions of the original crime.

Cyber Laws around the world are crafted to be as widely applicable as possible to respond to the rapidly changing technology landscape. This overreaching makes it confusing for local developers to understand what is, and is not, illegal. The United Arab Emirates case is also a good example of this. After they updated the law in 2016 to increase the severity of its fines there was widespread confusion about how it applied to legitimate businesses and professionals who rely on VPNs to protect their internet traffic from corporate espionage and hackers. The Telecommunication Regulatory Authority had to eventually respond to these complaints with a follow-up statement.

> "Telecommunication Regulatory Authority issued a [statement] vowing that the law will not affect economic interests, and promising that business can continue to use VPN technology on their internal networks, as long as they don't misuse it for criminal activities." - Advox, Global Voices[42]

Collaboration between IHRFGs and local developers should take the broadness and compounding effect of local Cyber Laws into account when designing collaborations. If these laws are a concern IHRFGs should work with the local developer to reduce the possibility of them being targeted and identify local legal aid resources to ensure that the local developer has legal support if they are.

Extrajudicial Sanctioning

The types activities that make one "applicable for sanctioning" are far more varied in areas where security forces are given widespread autonomy to extrajudicially target and carry out sanctioning as well as in situations where the sanctioning is coming from powerful non-governmental actors such as organized criminal enterprises. In these environments the likelihood of sanctioning becomes more common and its severity significantly increases.

IHRFGs and local developers looking to collaborate in these types of environments should be especially mindful of the historic risk landscape for these types of activities. If local actors are routinely or arbitrarily sanctioned the way collaboration is done with local developers will have

[41] Individuals can access VPNs in UAE - https://web.archive.org/web/20170426131411/http://gulfnews.com/business/sectors/technology/individuals-can-access-vpns-in-uae-1.1872304

[42] Bad Laws Are Contagious: Demystifying the UAE's New Information Tech Law - https://advox.globalvoices.org/2016/08/03/bad-laws-are-contagious-demystifying-the-uaes-new-information-tech-law/

to be carefully orchestrated to help ensure that they are not associated with the activities and technology. By maintaining strict processes around maintaining their anonymity or pseudo-anonymity local developers can significantly reduce the likelihood of being arbitrarily targeted and severely sanctioned.

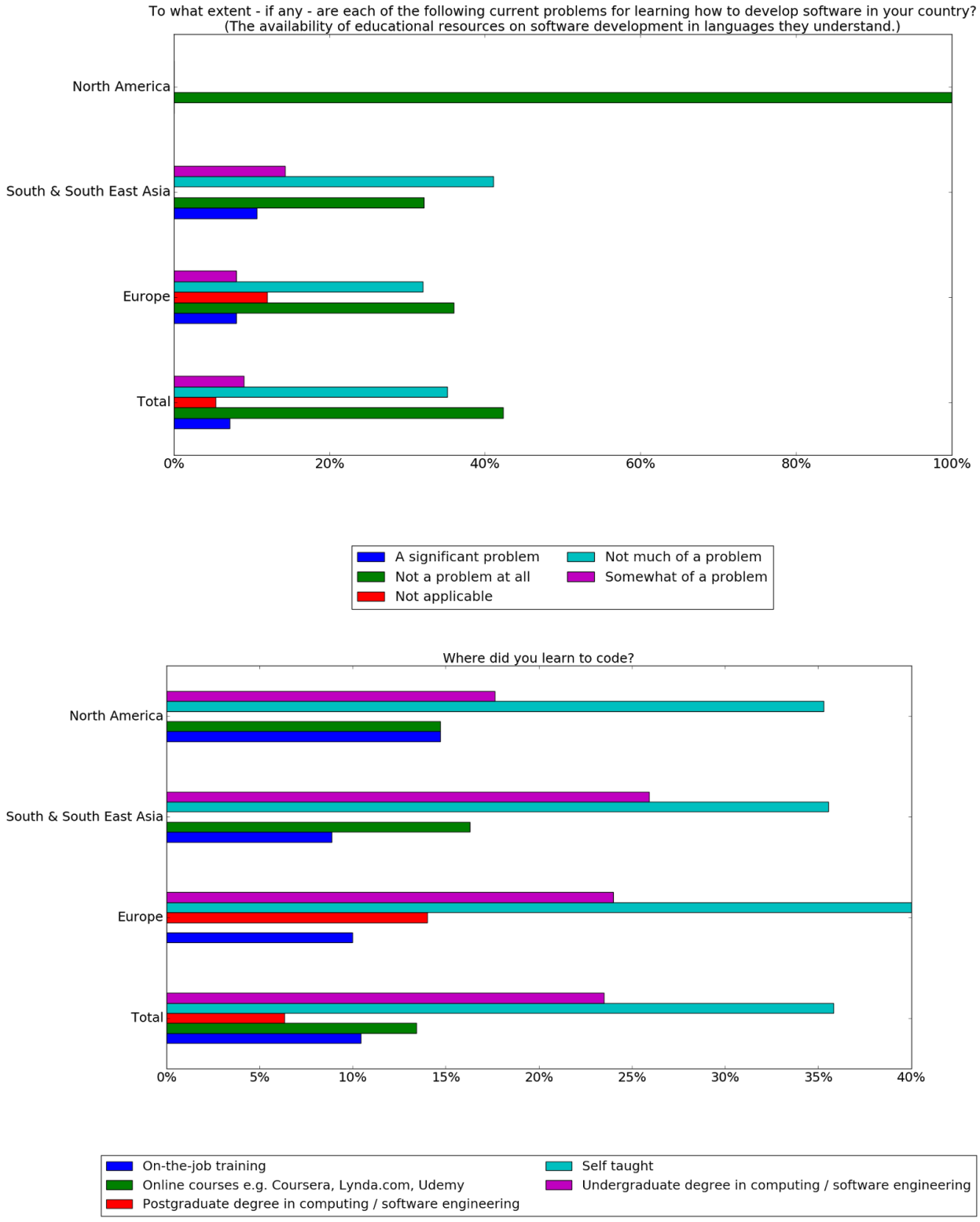
Developers Worldwide

There are developer specific challenges that international groups who support Human Rights and freedom (IHRFGs) should take into consideration when looking to build greater collaboration with local developers. Language barriers often make it difficult for interested local developers to find IHRFG projects that might serve their purposes, and technical communities that they would benefit from joining. Technology focused IHRFG communities and local technical communities often have a mutual lack of knowledge of, and transparency into, the foundational principles, use-cases, and best-practices that have been developed in their respective communities. This creates the possibility of misunderstanding and disagreement. It also creates a valuable opportunity for each community to understand and assimilate the valuable aspects of each other's knowledge into their work.

Language Barriers

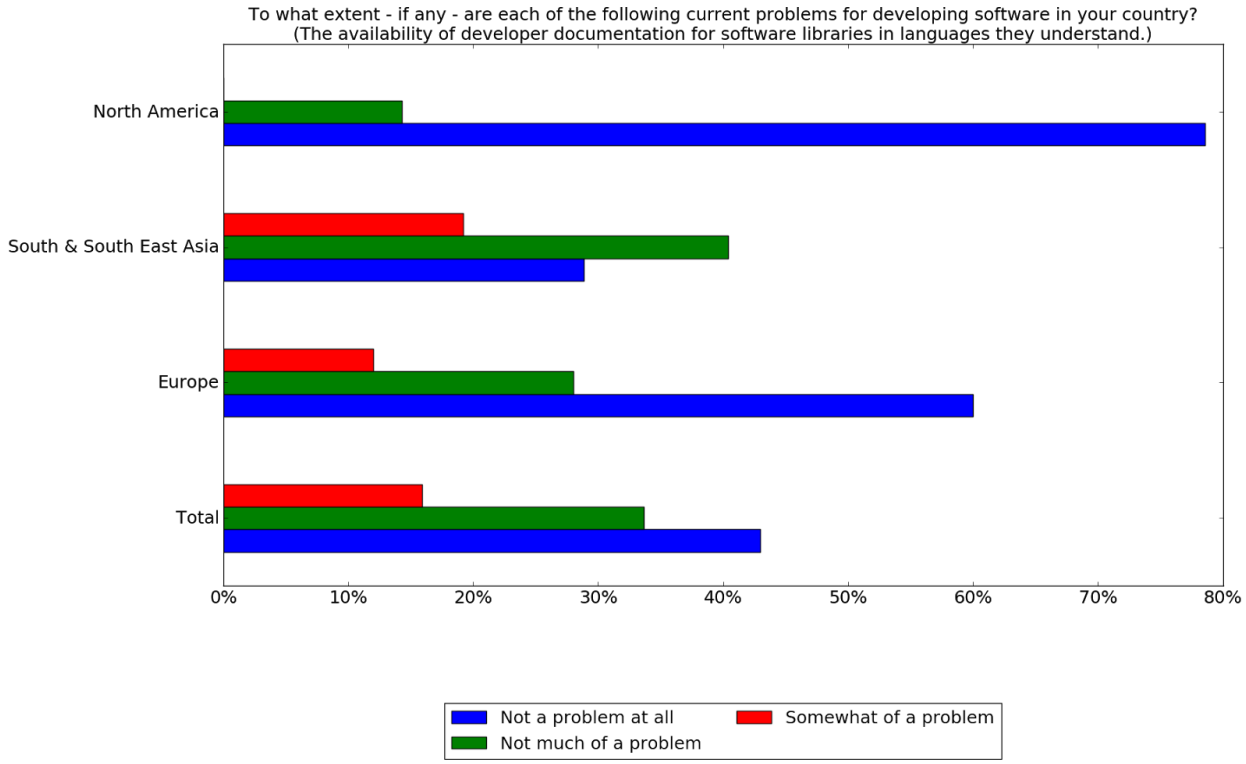
English is the “lingua franca” of technology.[43,44,45] It is so ubiquitous that more than a few of the individuals that we interviewed noted that basic english literacy is a baseline requirement for becoming a developer. Almost all programming languages use English keywords[46]; software documentation is rarely translated into other languages, and when it is, it can take significant time for translated documentation to catch up with current versions of the software; and the largest share of programming educational resources available is in English.

[43] Why English is really important to us non-english speakers. - https://web.archive.org/web/20150318205057/http://blogs.lessthandot.com/index.php/architect/designingsoftware/why-english-is-really-important-to-us-no/
[44]Do you have to know English to be a Programmer? - http://www.hanselman.com/blog/DoYouHaveToKnowEnglishToBeAProgrammer.aspx
[45] The Ugly American Programmer- https://blog.codinghorror.com/the-ugly-american-programmer/
[46] Non-English-based programming languages - https://en.wikipedia.org/wiki/Non-English-based_programming_languages



Developers around the world often have learned to read *technical* English as a second language (ESL). This language barrier means that developers do not actively engage in English language

development communities. The challenge of translating their questions into English, and disinterest in dealing with the sometimes harsh response to their translations can cause them to spend much more time crafting their messages, and be overall less willing to engage in primarily English fora at all. As such, reading documentation is often the primary way ESL developers evaluate if software meets their needs, and is worth investing time into.



Open-source IHRFGs software projects often dedicate their limited resources to user-facing functionality, features, and documentation instead of developer facing informational and educational resources. Developer facing resources are often sub-par, or non-existent in the open-source IHRFGs software space as a result of this. IHRFG software projects that are looking to grow their international developer bases need to dedicate resources towards improving the accessibility and utility of their developer facing resources for international developers.

Much of what makes identifying and evaluating a software project easier for international developers revolves around the language the software project uses. There are 3 primary types of language that a developer uses to to evaluate if software meets their needs, and is worth investing time into:

1. The language about a software project that is indexed by search engines;

2. The introductory language that describes what problems a piece of software solves, what differentiates it from its alternatives, and guides a developer through basic installation and use; and
3. the language in the full technical documentation.

Language for search engines

Identifying software libraries requires a certain level of comfort with the domain specific language of that technology. A developer looking for the right type of software must first be able to

- identify and understand the terms that describe “what” they are securing communications from,
- identify and understand the terms for the appropriate methods for accomplishing that,
- identify and understand the terms that describe required subcomponents of these methods needed to evaluate if a piece of software that claims to provide a method actually does, and
- use those terms to seek out and evaluate existing software libraries.

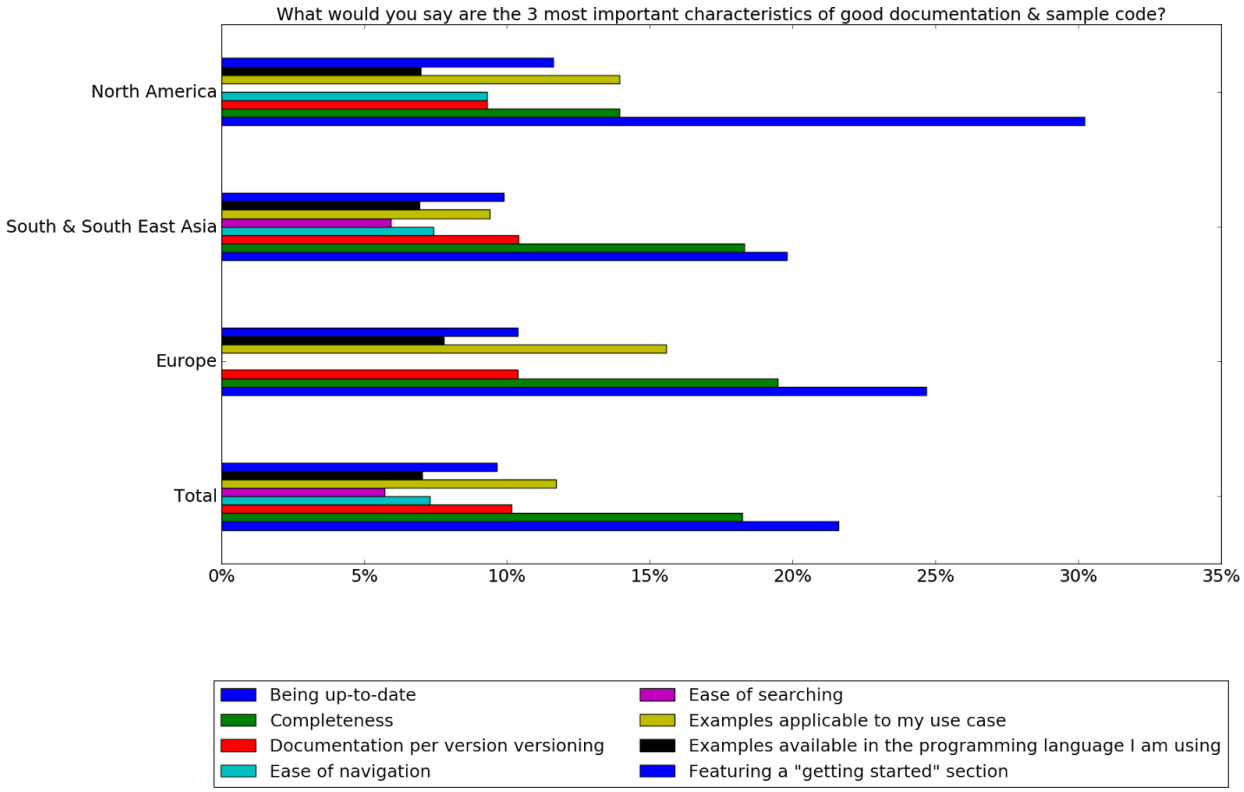
For example, there are hundreds of different types of software libraries for “securing communications.” If a developer want to secure their users communication from “passive eavesdropping” “on the wire” but they also wish to filter malware from messages they need “client-to-server” encryption. If they wanted to provide users communications that are secure from anyone including themselves they need “end-to-end” encryption. Both “client-to-server” and “end-to-end” encryption can be implemented using a variety of protocols. Each of these individual protocols are often implemented in multiple software libraries. When a developer is searching for a software solution that meets their projects needs “secure communications” is only the first, of many terms they need to understand to be able to evaluate in a piece of software.

IHRFG software project need to provide multiple levels of language that allow their project to be easily found and evaluated by ESL developers. The traditional focus on, highly accurate, domain specific language makes it difficult for IHRFG projects to be identified by developers who are not a part of the IHRFG technology community and, by operating in a second language, will have greater difficulty identifying the domain specific terms needed to find these tools from the “mass-market” technology texts that are available to them.

Introductory Language

When a developer is evaluating a variety of open-source software projects to see if they serve their use-case they only have time to explore a subset of those projects deeply. Developer use a project's summary and introductory documentation to identify projects for further exploration.

This documentation describes what problems a piece of software solves, what differentiates it from its alternatives, and guides a developer through basic installation and use,



Most ESL developers have focused on building their comprehension of technical English. This allows them to read technical documentation, but often does not prepare them for complex conversational and narrative english. The summary and introductory documentation for software projects is often written in conversational English. This documentation uses narratives, idioms, and complex sentences to describe the project. It is quickly written, rarely translated, and describes use cases that are deeply rooted in the original developers context. Evaluating projects based upon such casually written narratives can be difficult for ESL developers have vastly different use-cases than the original author.

Technical Documentation

Translating core developer documentation is a difficult task. IHRFGs will have to find a competent translator who can both translate between the languages and understand the software and its technical context. Mis-translations of developer documentation can be so misleading that it can prevent developers from successfully using the software, or lead them to use the software inappropriately. When the software in question is being used with vulnerable or at-risk populations this can have severe consequences.

For IHRFG software projects with limited resources localization should start with introductory and narrative elements of the software. Technical documentation should focus on producing clear, concise technical English. When translation is done on technical documentation it should be evaluated by a developer who speaks the language in question, and has used the software in their own development projects.

Support Networks

Only a subset of English language technical resources are translated into other languages. When international publishers choose to translate a resource, they only translate it into a small number of languages. Even fewer online English language resources, such as blog postings by software projects and industry experts, are ever translated. There are, of course, local language online technical communities in a range of languages that are widely and actively used by local developers.

The topical focus and culture of online technical communities differs across different language communities. They are driven by the availability of existing expertise within a community, shared use-cases for the technology, and cultural and environmental factors that determine acceptable behavior and topics for discussion. Over time, these incidental community focuses and behaviors become codified principles that differentiate the behavior and priorities of developer communities all over the world.

This is not to say that there are not a variety of principles that are shared internationally across various communities. Internationally shared principles do frequently occur around international communities that come together to address specific shared use-cases[47] or technically focused best-practices[48].

The number of international technology focused IHRFG communities is relatively small. The likelihood that a IHRFG finds a local developer who is an active member, or even aware, of these communities is unlikely. Like any technical community international IHRFG technical communities have their own deeply held principles. When an IHRFG and a local developer first start to engage in collaboration their mutual lack of knowledge of, transparency into, and access to their respective communities means that there is a possibility of misunderstanding and disagreements based upon divergent principles. Not only can this cause interpersonal conflict among experts from different communities, if assumptions are made about how security will be implemented or verified; how technology will be implemented; how licensing, copyright, or source-code access/ownership will be handled; or who will handle maintenance of the services created conflict can easily disrupt or derail a project.

[47] Pluggable Transports - https://www.pluggabletransports.info/
[48] The Cryptography and Cryptography Policy Mailing List - http://www.metzdowd.com/mailman/listinfo/cryptography

The divergent principles of local developers and IHRFGs offer more than just challenges to their collaborations. Output focused collaborations can create IHRFG services and software that are built on global best practices around IHRFG technology implementation while being responsive to the context and use-cases of the local environment. The long-term value of engagements that open up channels between local technical communities and technical IHRFG communities can not be overstated. They can offer long-term benefits when each community takes the opportunity to understand and assimilate the valuable aspects of each other's knowledge into their work. When IHRFGs participate in the online fora or local events of regional technical communities they increase awareness of IHRFG software projects and best practices. This creates opportunities for local technical communities to assimilate IHRFG principles and practices that they find useful into their work, and for IHRFGs to localize their software based upon the principles and practices of local technical communities. This will create software that local developers can easily incorporate into their projects and will better suit their needs.

Key Insights & Recommendations

For all international groups who support Human Rights and freedom (IHRFGs)

1. IHRFGs should collaborate with local developers whenever possible.
2. IHRFGs should engage with local developers from the earliest possible stages of project design. Local developers have valuable understandings of the local context and can make an IHRFGs work far more successful and sustainable.
    a. This is especially true when it comes to assessing and mitigating the possible risks of a project in closed and closing spaces or when working with at-risk or vulnerable populations. IHRFGs should include local developer partners when developing the relevant parts of their risk assessments. Each party's individual expertise provides them a unique understanding of the possible risks. This will help ensure that both the IHRFG and local developer partner has a more complete understanding of the actual risks, and are appropriately mitigating those risks.
3. Programs should be designed to build the capacity of local developer communities to sustainably build software and services that are targeted to their local regions needs and markets. Examples of this include:
    a. Create strategic fellowships and skill-building programs for local developers that provide
        i. Introductions and access to international technology communities;
        ii. financial resources to support them during that period;
        iii. guidance on how to build appropriate and sustainable business models in their region;
    b. Fund the translation of technology and security resources that are relevant to the local context or the creation of localized versions of similar resources.
4. Support local advocacy and policy efforts aimed at building greater consumer protections around technology. Consumer protection laws are critical to the healthy development of a local technology sector and are becoming increasingly important as technology and data sovereignty continue to push developers to local technological markets.

For international Software Projects in support of Human Rights and freedom

1. Provide concise technical introductions that describe what the software project does, what problems it solves, and how it can be used. This will make it easier for unfamiliar developers to evaluate your software for their purposes. Translate this introductory documentation into other languages when you translate your user documentation.
2. When writing technical and explanatory documentation for software projects
    - use simple, clear language and grammar;
    - provide a glossary that defines key concepts and technical terms or provide links to external resources that do so;
    - avoid the use of idioms or metaphors;
    - describe your project, and the problems it solves, using language from multiple levels of expertise so that it can be more easily found in online searches; and
    - seek out and provide a range of use-cases for your software pulled from international developer communities.
3. Allow (pseudo)-anonymous contributions to your project. Provide clear contribution guidelines for (pseudo)-anonymous contributions. These guidelines should provide guidance on the steps a developer should follow to ensure their (pseudo)-anonymity and ways the project can provide additional guidance to ensure their success or make the process easier.
4. Where possible, provide links to the online profiles (github, facebook, blogs, etc) of the development team so that higher-risk developers can evaluate the legitimacy and trustworthiness of the projects members before reaching out.
5. Be mindful of the different levels of access to IHRFG security best practices and the varying prioritization of security around the world when interacting with the developer community. Treating members of online spaces with, seemingly, incorrect opinions about security, with dismissiveness, disrespect, or hostility will likely drive away possible collaboration with developers from areas that would benefit from your projects adoption.
6. Provide introductions between the local developers who you collaborate with and international technology spaces (forums, list-servs, etc.) that you participate in. These spaces can be difficult to identify from outside of their respective communities.

Appendix A: Developer Profiles

The following personas were developed to help readers better understand the motivations and challenges identified by the interview participants. In designing collaborations or looking to support local developers, personas can help IHRFGs think more concretely about how to best support these activities.

Auður Gunnarsson - The Open Source Contributor

Background

Auður is a 31 year old developer who does database administration for a living, and contributes to open-source software development in both her professional and personal time. Auður started contributing to open-source software when she found and fixed a bug in the open-source database software she uses at work. Over time, as she continued to find and fix bugs and add features that she needed at work she became a core member of the project. She has also contributed code to a variety of other international software projects that ask for help. Auður participates in a variety of international technology focused list-servs, IRC chatrooms, and forums in her professional capacity and under her real name.

Motivations

Auður has become increasingly worried about the level of corruption in her government. She has also watched suppression of free speech and the media increase since the new president took power. Auður does not participate in the public protests that have started to become more commonplace recently, but she does spend a lot of time talking on social media about how horrible the government has become.

Collaboration

Last year she heard about a secure and anonymous chat application for activists. When she went to the website she noticed that it was using her database on the backend. Auður could tell by the code that they did not have much experience working with the database and decided she had to contribute.

Challenges

- There are no formal laws against contributing to security tools in her country. But, the government has made public statements that those tools are made and used for terrorism. All the public cases where citizens were tried for terrorism related activities, that Auður knows about, led them to life sentences or those individuals disappearing from prison. Auður was very cautious when it came to trying to contribute to the secure chat application.

- Auður decided to create a new online handle to contribute to this project. Her “handles” lack of an online history made her initial interactions with the projects members difficult. When Auður asked if the tool could protect activists from government surveillance on their IRC the

developers would not provide answers to her questions, They were concerned that Auður was an “intelligence agency plant” from their own government who was running a sting operation against them.

- Auður decided that she would contribute to the project to gain their trust. She went over their database code and made a series of changes to increase its speed. When she submitted the fixes they were rejected because the developer team did not have the time to review such as extensive amount of changes. They joked on IRC that this is exactly the kind of code contribution where backdoors are hidden. Auður was disheartened, since her contributions, while changing many lines of code, were the kind of code contribution she would be happy to accept in the codebase she manages. It took a series of of small and heavily documented contributions for the projects team to start to trust Auður to contribute more code. She now makes occasional contributions to the code to fix issues that she and her friends encounter.

Soraya Herce - The Circumvention Supplier

Background

Soraya is a 28 year old developer who makes a living selling in-app advertising and subscriptions in a few different Virtual Private Network (VPN) apps she has developed.

The country that Soraya lives in has widespread, and pervasive, internet censorship. Nearly every citizen uses some form of circumvention app so that they can access social media sites. The government, knowing this, frequently attempts to block circumvention tools that it identifies. As the government prevents one app from working citizens respond by changing to other circumvention apps.

Soraya releases her apps in both the Google Play store and in a few locally popular App Stores. A majority of her new customers get their app when she gives it to them, or when it is sent to them by one of xer other customers when they are looking for a new circumvention tool. Her customer base ebbs and flows depending upon whether or not her app is working when one of her competitors apps gets blocked by recent changes in censorship.

Motivations

Soraya likes the feeling of being relied on to help those around her. Soraya codes circumvention apps because she likes the challenge. She finds network code interesting and likes to spend an evening puzzling over how to get around the latest changes in the government firewalls. There are few greater joys for Soraya than being able to announce that she is the first app that is updated to get around the latest blocks.

Challenges

- Even though circumvention tools are illegal she does not think that she is doing anything wrong. There is extensive use of censorship circumvention software and Soraya has never heard of anyone being targeted because they were using circumvention software. Soraya's friends have told her that she will probably only be targeted if the government starts a public-facing effort to "crackdown" on circumvention. Even though it is unlikely, Soraya guesses that if she is targeted the punishment would likely be severe because it would be a part of "security theatre" that shows that the government is taking the issue of illegal circumvention seriously. Earlier this year the government made a point of arresting a developer who built a secure chat app because it was used by terrorists.
- Soraya keeps getting negative reviews on her app in the app store because

Photo Placeit - Unlimited License

it does not have the perfect security that western security professionals want. She is getting tired of having to respond to the “NSA digital security requirements.” Soraya’s users care far more about getting access to the internet than they do about protecting their communications from being monitored. She is not going to put a lot of time into additional security that a majority of her users don’t need, and could slow down the speed of her app.

Aregnazan Kocharyan - The Game Developer

Background

Aregnazan is a 45 year old developer who builds works on mobile app development for a regional bank. Aregnazan got a job in the banks IT department out of college and got hired by their development team after teaching herself mobile app development in the evenings. Aregnazan is married and has a five year old son.

Aregnazan's country has had strict foreign exchange controls in place for a few years now. This makes it nearly impossible for anyone to transfer money in and out of the country. The foreign exchange controls compounded the country's historically low income levels to make matters even worse for citizens.

Like many, current conditions requires that Aregnazan get income from a few different sources. Aregnazan has been developing and selling mobile games in her free time. She sells them in a local Ahpp store and splits the profits with a local mobile phone retailer who sells app install in their store.

Motivations

Aregnazan is most motivated by her family. Her partner and son are the most important things in her life. While maintaining the banks app is a boring job Aregnazan considers herself lucky to have a stable job that allows her to take care of her family.

Aregnazan loves playing and developing mobile games in her free time. She aspires to make a living selling mobile games. When Aregnazan manager became one of her customers they tole her that she would be fired if she released any financial apps that compete with the banks. Aregnazan has no intention of jeopardizing their job, and ability to take care of their family, by building a competing app.

Challenges

- There are no opportunities to pursue international mobile development freelancing or remote work besides the bank because the foreign exchange controls make it nearly impossible to exchange foreign currency into local currency.

- While Aregnazan has dreams of developing mobile games full time there is no way she can do it and continue to support her family. The app markets are not big enough in her local region to make a living of game sames. Even if they could make enough money through app sales, in-app purchases, or advertising in international App stores the foreign exchange controls would prevent her from getting access to that money. Aregnazan's son was born right before the currency controls were put in place.

Aregnazan had considered fleeing the country to get a higher paying job and eventually bring her family out with her. But, once the currency controls were put in place it would have been impossible for her to send back money to support her family while she was away.

- Aregnazan has occasionally found some of her games on a local software piracy websites. She was worried that this would wipe out the small amount of extra profit that this was bringing into their house. Luckily, when Aregnazan reached out to the owners of the web-sites they were happy to remove the app because she was local. Aregnazan now searches through these sites once or twice a week to try and catch any new uploads and get them taken down.

Marnix Van Dongen - The Human Rights Newcomer

Background

Marnix is a 22 year old web-developer and part-time computer science student who is deeply passionate about Free Software and software development for the social good. Marnix uses an online freelancing websites to find new clients to contract with.

There is widespread and systemic abuse and corruption perpetrated by local authorities in the region where Marnix lives. People frequently have to provide bribes in exchange for basic government services and can face ongoing extortion if they are targeted by local authorities.

Motivations

Marnix got into technology because there are limited local opportunities to make money and technology seemed like it would allow him to make a living without having to leave his family to go abroad. As Marnix became more politically active he started to volunteer by setting up websites and blogs for advocacy groups on their campus.

Collaboration

One of Marnix's previous clients sent him an email with a posting by an international Human Rights organization looking to hire a local developer. The organization wants a local developer to build and maintain a website to accompany an advocacy project they are running. The website will allow sex workers to crowdsource incidents of abuse and extortion by local police.

Marnix was excited about the technical challenge, high pay, and possible positive impact if he got the project. But, he was also concerned. Marnix had never worked on a project with this large of a public presence and did not know what the repercussions might be for taking part in a project that was so antagonistic towards local police.

Challenges

- Marnix does not know if there will be repercussions for creating this software. Marnix does know that he needs the work. Even with the international freelance work there is only ever enough work for him to scrape by. If this project was not offering as high pay as it was Marnix would never have agreed to take the risk.
- Marnix has an even more limited understanding of possible risks to the sex workers than he has for himself. For instance, Marnix has no idea that the police raided the offices of a different

NGO that was working with sex workers last year and confiscated their files; Or that they used those files to identify and arrest over twenty different individuals. Marnix will be creating a database that will be storing information and incident reports by sex workers as the backend of the crowdsourced data platform. Without guidance there is a distinct possibility that Marnix will collect enough information to allow a repeat of this incident on a much wider scale.

- The project was designed with an end date in mind. The international human rights organization knows that they are likely to not receive continued funding and does not plan to support the website after the project ends. They plan to simply leave the platform up so that they can use it in their communications and development materials. Marnix is contracted to maintain the platform throughout the project. When the project ends Marnix will have to make the hard choice of continuing to maintain this valuable local resource for free so that it is still useful for sex workers or letting it decay, and possibly be compromised, because he is no longer being paid. This will be a difficult choice for Marnix because he believes that the project can continue to do a lot of good.

Virve Orav - The Entrepreneur

Background

Virve is a 48 year old developer who runs a cloud based log management service for IT professionals. She used to worked in IT for a multinational company. After a few years she and decided to take the system she had built to centralize log management for that company and start selling it as a service. She now runs her own company alongside her partner who focuses on sales.

A year ago a series of technology sovereignty laws were implemented in her country. These laws require businesses to use in-country servers to store and process data about their citizens. As one of the few log-management services that was able to quickly find and start using in-country servers this led to a spike in her business. This increase in business allowed Virve to hire an employee whose job has mostly been taken up with managing challenges related to the in-country hosting.

Motivations

Virve's primary goal is to make a decent living and to be her own boss. Virve likes that her business partner deals with the clients so she can focus on making their service better.

Challenges

- The recent technological sovereignty laws require that Virve use local services for hosting and processing their citizens data. There is a local oligopoly of a few hosting providers. Since there are only a few companies who dominate the market they are have no reason to improve the quality of their services and in their security. Because of this, they are severely lacking in both.
- Log management requires massive consumption and processing of massive amounts of business data. Unlike the international hosting providers that Virve was using before the laws the local hosting providers have a variety of unstated limitations on their machines. Virve's continues to have situations where the servers start dropping client data when a previously unknown limit on the disk size or bandwidth of one of the local hosting providers is reached. This has become such a problem that there is now a collaboratively maintained spreadsheet floating around the local tech scene which lists the "real capabilities" of different local hosting providers.
- Last year one of the hosting providers sent out a plain text email to all of their clients that contained that client's username and passwords. This caused an outcry among local developers because

not hashing users passwords is an indicator that the hosting companies are not putting even basic security in place. The company released a statement that they were using “military grade crypto” for their login portal and that they would fix the problem. Virve is not convinced that they have, but has few options but to continue to use the service since she needs it as a redundancy for when the other hosting providers services fail.

- The lack of technology related consumer protection laws mean that Virve has little recourse when these things occur. Her business partner talked to a local lawyer who said that they didn’t think that they could get much in a lawsuit because the terms of service eschew nearly all liability and there is no precedence in the local courts.
- Virve has been losing local customers because hosting issues keep causing them to drop customer logs. Virve’s business partner is furious and has been pressuring her to do something to stop this from happening. Virve met up with other local developers to talk about how they provide services on the inconsistent local hosting providers. One of these developers suggested some methods for “working around the law” by strategically using a combination of international and local cloud services to provide decent services without raising suspicion of local authorities. They suggested setting up a local fallback proxy server that will send data from local servers to servers outside of the country when their hosting fails. This way the clients would still only see a local address and they could move the data back later when they addressed the problem. Even though would be a temporary measure, Virve is worried about the legality of this. Their lawyer thinks that the consequences would be low since they are just handling logs, but does not recommend that they move forward since it is technically illegal.

Norbert Bender - The Accidentally Essential Technologist

Background

Norbert is a 42 year old developer who does everything from IT to website development at an environmental advocacy non-governmental organization (NGO). Norbert started working at this NGO about 7 years ago as one of the administrative staff. After fixing the printer one time the staff started to rely more and more on Norbert for technical help. Norbert's job transitioned entirely to technology after Norbert created a website that allowed users to fill out a form to send emails to their local representative in favor of stricter controls on logging.

Norbert's NGO is actively targeted by the government because of their work. Many of the government officials in his country make illicit deals with logging and mining companies to harvest the country's vast natural resources. The expose's that Norbert's NGO has done over the last 10 years has embarrassed these officials and caused the organization and its more prominent staff members to become targets.

Motivations

Norbert cares deeply about the environment and the work that his NGO is doing. He has gotten very good at the technical aspects of his job and thinks that it makes their work more impactful.

Collaboration

It is illegal for NGOs in his country to take money from international donors to conduct political activities. Norbert's NGO is primarily funded by international donors. The organization is currently being run by its vice-president after the previous CEO was arrested on tax evasion charges. These charges were primarily based upon the various ways that the previous CEO had to launder the source of the NGOs funding to avoid being tried under the country's severe "foreign agent" laws. Norbert does not have anything to do with his organization's fundraising, but he has had to travel out of the country to show off their websites to their donors and to attend events with other censored web-developers that their donors fund to talk about methods for circumventing censorship.

Challenges

g * The content of his NGOs main website, and the websites of its campaigns, are deemed "harmful" by the government and are actively censored. He spends a lot of his time trying to circumvent that censorship. This is time consuming and, de-

pending upon how the site is blocked, it can be expensive.

- The “cyber laws” in his region allow for a range of extreme punishments for any type of violation. Norbert is increasingly worried about his role in circumventing the government’s censorship. While the original content is not illegal, the censorship circumvention that he is conducting is illegal under the local cyber laws. Since Norbert’s NGO has moved primarily to online campaigns and he is the only developer Norbert is worried that he might be targeted to stop the organization from being able to do its work.

- Norbert’s concerns about being targeted by government officials has made him wary of being recognized for his work. Norbert works very hard to not be the focus of public attention for his NGO. Norbert intentionally left his bio and picture off of the staff page of the NGOs website. Norbert is pseudo-anonymously a member of a variety of local listservs and forums. He uses these to reads up on new ways to get around local censorship and to share the methods that he uses. He uses an “online handle” and never reveals his identity when using these sites. Norbert is worried that it could be used against him by authorities in the future. He does have some very close friends he met at a local hackerspace. He will talk to them about problems he is facing. But, Norbert only ever does it in person because he does not want to leave a paper trail.

- Norbert’s copy of windows and all his website development and design software is pirated because he cannot afford to purchase it legally. Since their NGO started being actively targeted by the government for their work he has started to worry that this pirated software makes his computer insecure. He is primarily worried about the security of the private keys and passwords that he uses to access the different websites sites & development projects for his NGO. Norbert has looked online for how to protect himself, but the advice given is always just for her to buy legal copies of the software.