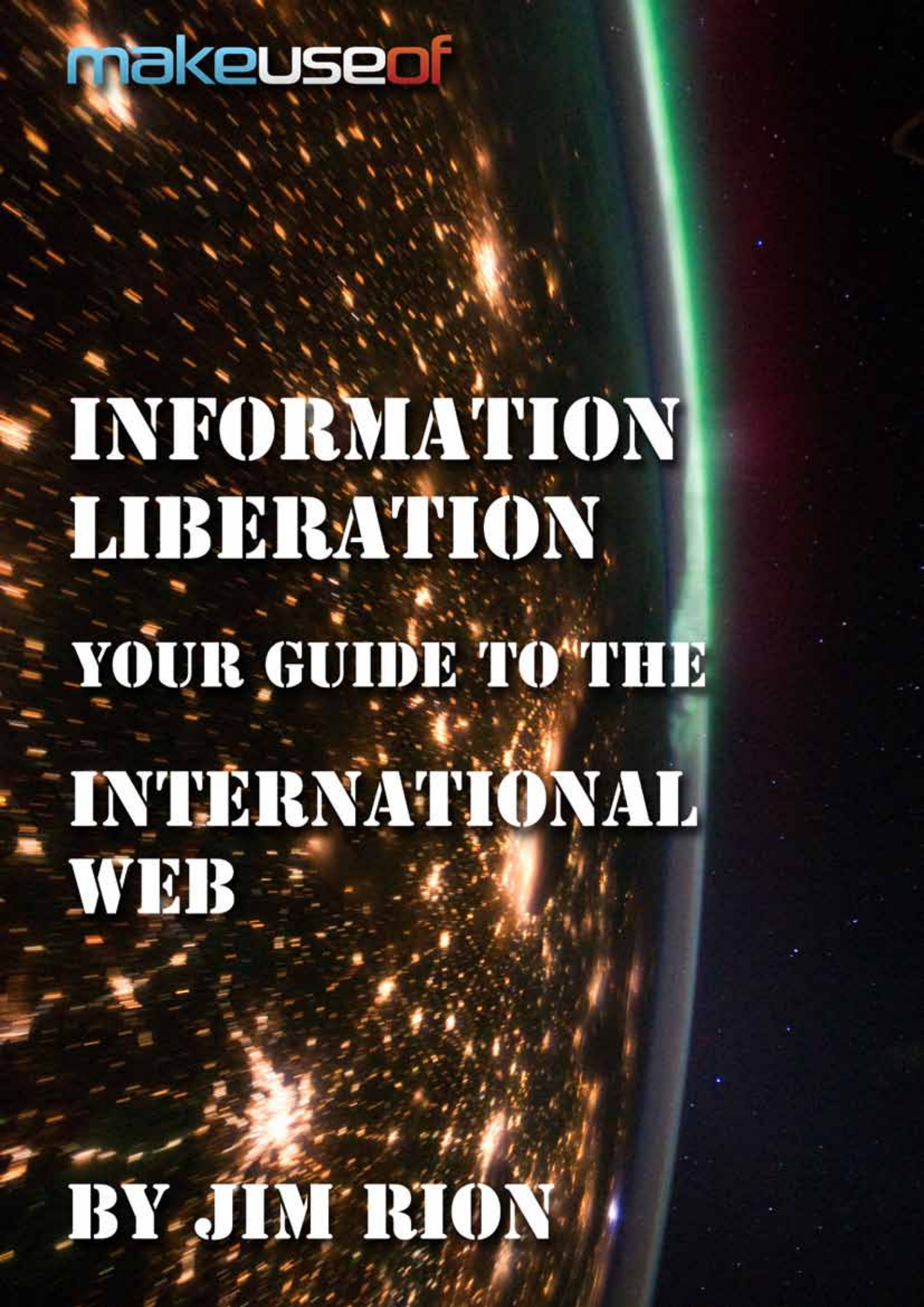

makeuseof
INFORMATION LIBERATION
YOUR GUIDE TO THE INTERNATIONAL WEB
BY JIM RION

By Jim Rion

JimRion.com

Edited by Justin Pot

Table Of Contents

Foreword **6**

1. Government and the Net **7**

1. North Korea. 7

2. China 8

3. Iran 8

4. Saudi Arabia 8

Lesser known censorship 9

Should We Bypass This Censorship? 9

Consequences Of Bypassing National Censors 10

Ethics Of Illegal Bypassing 10

Web Tools & Human Rights Issues 11

Tools For Bypassing Internet Censorship 12

Data Security 13

Email Encryption 13

Disk & File Protection 14

2. International Netting Practicalities **15**

For The Traveler 15

Finding Access 15

Net Cafés & The Backpacker 15

Using Hotels, Hostels etc. 15

The Holy Grail: Free Wi-Fi 16

Online Sites 16

Likely Locations 16

Security 16

3. Special Notes For The Expat **18**

Setting Up a PC While Abroad 18

General Language Issues On The Net 19

Displaying Non-Alphabetic Languages 19

Translation Tools & How To Get The Most Out Of Them 20

4. Accessing Region-Blocked Media **21**

Region Locking & What It Means For You 21

VPNs, Tunneling & IPN Spoofing 21

Free Services 21

Paid Services 22

The Final Word **23**

Foreword

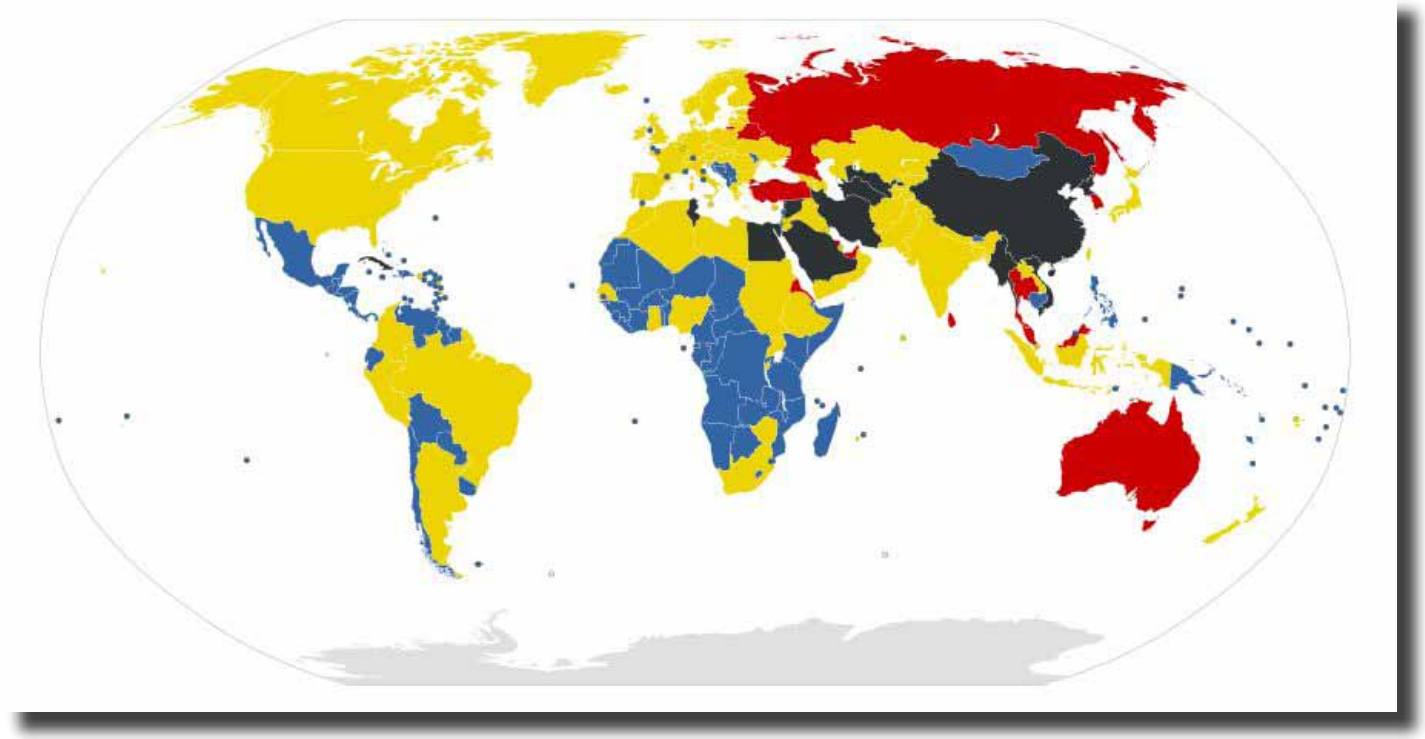
Few would argue, I think, that the Internet has not changed the world dramatically. Every day we see how free, instantaneous communication influences politics, social change, and daily interactions at a fundamental level. But even with all of this, there still remains a certain level of provincialism on the net - Americans stick to American websites; Japanese stick to Japanese websites; you get the idea.

Part of this, of course, is due to a simple language barrier; English is an international language, but it is by no means the only one. To some extent this artificial division of the web is by design. Media producers, like the BBC, often insist on restricting access to their products to certain geographical regions to protect their business models. Distributors (e.g. iTunes) are complicit in this, or even instigate it. Even worse, some governments insist on restricting Internet communication and blocking access to international websites.

This guide, then, is my small attempt at helping people deal with all of these problems. The Internet should connect people all over the world, not divide them. Whether you are a backpacker trying to check your email from a hostel in Denmark, or a college student trying to get past the Great Firewall of China, I hope there is some helpful information in here for you (though if you're reading this in China, I doubt you need any more help. Good job!).

1. Government and the Net

We're going to begin this guide with a discussion of the most vital issue: that of freedom of expression and governmental censorship of the Internet. This issue has become one of the most important of our time, due to any number of recent political events, and it certainly bears further discussion here. We'll look at some of the nations with the worst records in this regard, including a few of the lesser known offenders, and look at efforts people have taken to bypass the choking off of information. Of course, it will also be appropriate for us to discuss the ramifications, both good and bad, of those efforts.



National blocking or Censorship of the Net

The basic nature of the Internet — the pure transfer of information regardless of location — clearly creates a threat to groups (for instance, oppressive dictatorial regimes) that depend on a weak, ignorant populace for stability. Allowing people to know about the outside world might lead to an erosion of the very status quo that is so important to preserving illegitimate power. Obviously, true change comes from a variety of sources, and it would be foolish to overemphasize the role of the Internet in regime change like we have seen in the so-called "Arab Spring."

At the same time, the behavior of these regimes toward the Internet clearly implies the threat they see in it. Numerous nations, all of them repeatedly tainted by claims of human rights abuses and political corruption, take pains to restrict the free use of the Internet and often go as far as criminalizing efforts to bypass those restrictions. Of course, even that has not stopped people hungry for access to the world's information.

First, then, let's look at some of these countries and what they've done to deal with the problem of the Internet.

1. North Korea.

The Hermit Kingdom has done so much to earn its name; it almost boggles the mind. Information from within the nation is sparse: the occasional press release or intercepted television broadcast makes up the bulk of what we know about what happens inside North Korea. For an outsider, contact with an average North Korean citizen is almost completely unheard of. All of this is purely intentional on the part of the government, of course, so it should come as no surprise that, according to a 2010 New Yorker article, many North Korean citizens had never even heard of the Internet, much less had access to it (http://www.newyorker.com/reporting/2010/07/12/100712fa_fact_demick?currentPage=2).

There are apparently a few places, like hotels and PyongYang's only Internet café, where satellite Internet access is available — but only for non-citizens. According to a Korean Times article, Internet access is completely outlawed for private citizens of North Korea.

There are apparently government officials with Internet access, as there is an official North Korean Twitter account and YouTube channel, but for most of the businesses and government offices inside the nation the only access to a computer network is ""Kwangmyong," a national intranet connecting government offices, banks, financial institutions and other official entities. So, in other words, North Korea has designed its own, internal Internet reserved only for the elite.

2. China

China is, perhaps, the most famous of all nations on this list when it comes to filtering the Internet. In contrast with North Korea's near total lack of access, China boasts the largest number of Internet users in the world: around 513 million people there regularly access the Internet, more than the entire population of the USA. (That is still, however, only about 38% of the population — in the US nearly 80% of population has access).

One would think, with the Internet growing so quickly in China, that China would become increasingly connected to the rest of the world; but one would be wrong. The Chinese Internet is very much that: Chinese. Less than 6% of Chinese websites link outside of the country, and China's native search engine, Baidu, is far and away more popular than any international service.

The government is, naturally, deeply concerned with keeping this situation as it is. External Internet access is heavily censored, both incoming and outgoing. Chinese users are prevented from accessing external web addresses using a wide variety of techniques: DNS filtering and redirection, packet filtering, IP blocking and more. The effects are not absolute — there is some access to outside sites either by accident or design — but even then the government is watching. For example, a recent glitch opened up the Great Firewall to Google+, and users flooded President Obama's page with political comments criticizing the Chinese government and various policies. Voice of America questioned the Chinese Foreign Ministry spokesman Hong Lei:

"He repeated Beijing's position that it protects Chinese citizens' rights to free expression on the Internet. But he also warned that they should express themselves according to Chinese laws and regulations. "

Free, but…

3. Iran

Iran has a long history of Internet blocking and censorship; there are records of the government choking incoming Internet access points as far back as 2001. (http://opennet.net/research/profiles/iran#footnote16_bnup288). The early weeks of 2012, though, have seen a large upswing in Internet censorship, with access to the secure HTTPS protocol on external sites (such as Gmail) restricted, forcing users to log into external services without the extra layers of privacy and security encryption offers.

Watchdogs like the EFF and OpenNet Initiative see this escalation as a big step towards what one Iranian official has called the "Halal Internet," (http://www.fastcompany.com/1748123/iran-launching-halal-Internet) a national network focused on commerce and business and strongly guarded against "inappropriate" content — similar to the North Korean "Kwangmyong" network.

In addition to technological attempts to control Internet speech, of course, there are the more direct controls: bloggers and online activists are routinely detained, harassed and arrested for expressing views critical of the regime or otherwise unwelcome ideas online. Net cafes are required by law to have security cameras to record users' visits, and also record their browsing history and personal usage information for each computer used. (https://www.eff.org/deeplinks/2012/01/iran-escalates-campaign-against-online-expression) The atmosphere of control is near absolute.

4. Saudi Arabia

Not to be outdone by nearby Iran, Saudi Arabia filters a broad spectrum of content. Much like Iran, Saudi Arabia maintains a policy of jailing those who use the Internet for anything smelling of "subversion." A religious motivation is clear: much of the filtering is aimed at sites or content that register as "immoral" in the strict Sunni nation: homosexual, women's rights or pornographic content are all blocked, as are sites containing criticism of the Saudi regime or Islam.

Unlike China, which denies censorship when directly asked about it, censorship is openly acknowledged by the Saudi

Arabian "Internet Services Unit," the agency in charge of Internet filtering. You can see for yourself at their English language website: http://www.isu.net.sa/saudi-Internet/contenet-filtring/filtring.htm. I really recommend you read that page: it outlines some very interesting justifications for the suppression of free speech and information.

Lesser known censorship

The countries above are well known, and fairly open, about their control of information. It really shouldn't come as any surprise that Iran filters web content, or that North Korea keeps most people offline altogether. However, there are other countries which, while not infamous for online censorship, are still worth mentioning.

Burma (also known as Myanmar), is certainly worth consideration here. Internet access there is extremely limited (less than 1% of people have any kind of access to the Internet) due to economic and political reasons, but the government has announced plans to increase access throughout the country.

It did, in fact, lead to wider use of the net for the people of Burma, but there was a catch. In 2007, during a period of strong civil unrest and harsh military crackdowns, the Internet was used to disseminate information about the government's mistreatment of its people. The government's response was to completely shut the net down. (http://opennet.net/research/profiles/burma)

The country has shown some improvement since transitioning to a new government in 2011, but information about what's going on there now is still hard to find.

Turkey is also increasingly prominent in the free-web discussion. It consistently blocks access to websites containing information unwelcome by the Turkish government. For example: sites pertaining to Turkish Kurdish populations or labor unions are blocked, as is YouTube on occasion. (http://opennet.net/research/profiles/turkey)

Italy might be a bit of a surprise on this list, but then again it also isn't known for its freedom from corruption or ill-government. In terms of Internet security and privacy, it hasn't reached the outrage-inducing levels of Iran or China, but at the same time there are laws on the books which seem completely out of place in a modern Western democracy.

For example, Internet cafes in Italy are required to take copies of users' passports and submit them, along with usage information, to police agencies. The same law requires a periodical, comprehensive list of all the people in the country who use mobile phones. (http://opennet.net/research/profiles/italy#footnote31_2lc1tzf)

No bloggers are being thrown in jail, but Italy is not exactly a bastion for Internet freedom.

"Reporters without Borders" (http://en.rsf.org/) releases a yearly report on "Enemies of the Internet" which has invaluable information about national censorship of the Internet. It's available this year at: http://march12.rsf.org/en/#ccenemies. I encourage you to read it; it has some surprising information.

Should We Bypass This Censorship?

Having seen how so many countries are engaged in filtering and monitoring Internet usage within their borders whilst blocking content from outside, the natural inclination for geeks and activists alike is to start looking for ways around it. The fundamental freedom of the Internet, with its immediacy and its ubiquity, has become something of a given for so many of us that it would be hard to imagine constraining it.

Of course, in an oppressive regime like that of Iran, the obvious value of being able to exchange information freely with common citizens around the world, as well as exposing the harsh realities of life under such conditions, should make anyone try to find ways to break through government controls.

But is that the right thing to do? I'd like to look at that question in more depth here.

Consequences Of Bypassing National Censors

First, it is vital to consider the ramifications of breaking national filtering regulations. The ideal way would be to be to do so anonymously and have the freedom to communicate with no fear of repercussions, but the reality is that anonymizing services like TOR aren't perfect. There are often ways for authorities to find out who is saying what without permission. Then, of course, comes punishment.

Breaking the law in a country with strict Internet filtering is no joking matter. It is no coincidence that the same countries which appear on the lists of the worst Internet censors are also the same countries with repeated and persistent accusations of human rights abuses. Oppressive censorship is, in fact, a human rights abuse.

According to a BBC report filed in 2005, bloggers have been beaten and tortured for voicing things that the Iranian government found unacceptable. (http://news.bbc.co.uk/2/hi/technology/4283231.stm) China also has a long record of jailing Internet-based dissidents (http://en.rsf.org/chine-arrests-trials-and-sentences-offer-26-12-2011,39918.html, http://opennet.net/research/profiles/china#footnote175_cn3nbul) as does Saudi Arabia.

The consequences are thus very serious for those wanting to use the Internet to be heard. Is it worth it? Consider this seriously before bypassing any filter.

Ethics Of Illegal Bypassing

Oppressing freedom of speech online is not done in a vacuum: it is typically one part of a general oppression of human rights. The nations with the strongest filtering and monitoring systems are those with the worst records regarding the treatment of their own citizens. Often, exposing that mistreatment and making the realities of oppressive regimes public is one real step toward bringing them down.

The government of Burma knows this. That's why it took down all access to the Internet in 2007 - to prevent its people from telling the world what it was doing. That's why North Korea and Iran want to create their own, wholly domestic networks.

The "Arab Spring" of 2011 demonstrated that the Internet can have a (limited yet real) role in revolution, though of course the real work of liberation is done by real people, spilling real blood —that should never be forgotten. (http://www.miller-mccune.com/politics/the-cascading-effects-of-the-arab-spring-28575/)

But the deep censorship and monitoring of the Internet as a medium of communication is an infringement of fundamental human right. Article 19 of the Universal Declaration of Human Rights states:

Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The United Nations adopted the Declaration in 1948, and every member state has agreed to uphold it since then. (http://www.un.org/en/documents/udhr/)

So whether it is as a tool for organizing protests and exposing oppression to promote revolution, or simply as a basic expression of every human's right to freedom of expression, unfiltered access to the Internet as a means of communication with the world should be protected. Those who work to ensure that right, both inside and outside of these regimes, are freedom fighters and their work must continue.

Web Tools & Human Rights Issues

Now that we understand how important this work truly is, it is helpful to see what tools are most useful in the cause of Internet freedom.

As mentioned above, one of the most dramatic expressions of the Internet's new role in social and political activism is the Arab Spring. Beginning in early 2011, a series of demonstrations and crackdowns in cities across the Middle East and Northern Africa began an amazing series of domino-effect uprisings, leading to the downfall of regimes in Egypt, Libya, and Tunisia. The effects are still being felt, and at this moment the conflict rages on in Syria.

The role that the Internet played in this is still being hashed out, but (supposedly) one Cairo protester put it this way: "We use Facebook to schedule the protests, Twitter to co-ordinate, and YouTube to tell the world." The Internet is a tool for communication, and communication is vital for organized movements. It's as simple as that.

Twitter, as a tool for immediate, widespread communication, has obvious implications for freedom of expression and protest. The developers themselves openly value the role of free expression not only for its political usefulness but for its role in daily life.

From their blog:

Our goal is to instantly connect people everywhere to what is most meaningful to them. For this to happen, freedom of expression is essential. Some tweets may facilitate positive change in a repressed country, some make us laugh, some make us think, some downright anger a vast majority of users. We don't always agree with the things people choose to tweet, but we keep the information flowing irrespective of any view we may have about the content. (http://blog.twitter.com/2011/01/tweets-must-flow.html)

Government entities have repeatedly demanded Twitter censor or block certain tweets, and the company has been very resistant to those efforts, but recent changes have not been so freedom-friendly.

In January of 2012, Twitter enabled a nation-based system of tweet removal, so that tweets which have been deemed unacceptable by a certain country's regime can be removed from that country's twitter-sphere. This replaces a system where such tweets would disappear completely, for users in all countries. The French organization "Reporters Without Borders," which is a strong defender of free speech around the world, has come out publicly against this change. (http://en.rsf.org/dictators-can-thank-twitter-for-03-02-2012,41806.html). Others have been more positive.

Paul Smalera, deputy Opinion Editor for Reuters, wrote:

Twitter's policy and its transparency pledge with the censorship watchdog Chilling Effects is the most thoughtful, honest and realistic policy to come out of a technology company in a long time. Even an unsympathetic reading of the new censorship policy bears that out. (http://blogs.reuters.com/paulsmalera/2012/01/29/twitter's-censorship-is-a-gray-box-of-shame-but-not-for-twitter/)

Whatever side one comes down on, however, Twitter is clearly playing a major role in the Internet-freedom discussion.

Another battlefield for Internet freedom is the major search engines. Google's conflicts with the Chinese government are widely publicized. The biggest exchange came in 2010, when Google identified Chinese-backed hackers as the culprits in a series of attacks that year. (http://online.wsj.com/article/SB10001424052748704625004575090111817090670.html?mod=googlenews_wsj). This led Google to end its previous policy of self-censorship in accordance with the Chinese government's wishes, and directing searches from within China to its uncensored Hong Kong based search portal, Google.com.hk. (http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html) Since that time, Google has had no presence in mainland China, and there have been continued attacks from China-based hackers.

Microsoft Bing has had its own problems with Chinese influence on its searches, though in a different direction. Bing has partnered with China's leading search Engine, Baidu, giving it a huge step up over Google in the enormous Chinese market. (http://www.pcmag.com/article2/0,2817,2388087,00.asp). The cost, though, might have been high:

Microsoft respects and follows laws and regulations in every country where we run business. We operate in China in a manner that both respects local authority and culture and makes clear that we have differences of opinion with official content management policies. (http://www.nytimes.com/2011/07/05/technology/05microsoft.html?_r=1)

In other words, Microsoft will censor what China wants to censor, but not like it. This is not the only time Microsoft has had issues with Chinese censorship. In 2009, not long after MS first started dealing with Baidu and searches in China, many people noticed that whenever one used Bing in the Chinese language, regardless of location, "sensitive" topics like the Dalai Lama, Tiananmen Square, and human rights issues in China, were all censored. (http://kristof.blogs.nytimes.com/2009/06/24/microsoft-and-chinese-censorship/) At the time, Microsoft claimed this was a bug, but subsequently it became clear that this was an inevitable part of searching in Chinese. (http://kristof.blogs.nytimes.com/2009/11/20/boycott-microsoft-bing/). Either way, it seems somewhat….fishy.

Tools For Bypassing Internet Censorship

Besides the more obvious Internet tools, such as search engines and social networks, free speech on the Internet is also growing more dependent on tools that protect privacy and bypass some of the more pernicious elements of Internet blocking.

Tor (https://www.torproject.org/) is perhaps the best known, and most widely used, Internet anonymizing service. It's a tool based on US government work that has grown into a worldwide resource for those wishing to protect their identities while on the net.

Apart from the kind of dissidents and activists we've already discussed, Tor claims users in the intelligence field, journalism, corporate security and (of course) private users. Tor's privacy protection is not perfect; on their own website, they say:

Tor can't solve all anonymity problems. It focuses only on protecting the transport of data. You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information. For example, you can use Torbutton while browsing the web to withhold some information about your computer's configuration. Be aware that, like all anonymizing networks that are fast enough for web browsing, Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit. (https://www.torproject.org/about/overview.html.en#thesolution)

Tor itself is perhaps too visible, as now many elements of its software are specifically blocked in China, and Iran is targeting it as well. Tor's developers are dedicated to keeping up with the technology, though, and are developing new ways to help those under harsh restrictions to communicate freely. (http://www.zdnetasia.com/tor-anonymity-project-to-help-iranians-sidestep-net-ban-62303828.htm)

Other services with a similar function exist, of course, as well as more devious ways to bypass net filtering. It's a constant game of whack-a-mole for those in charge of blocking users from the net, and those exploiting gaps to help people get past the walls.

Services called VPNs (Virtual Private Networks) allow users in blocked countries to "tunnel" into an external ISP, meaning that their web experience is basically that of someone outside their borders. VPNs require a friendly server on the outside to run your Internet through. They also tend to be slow, but for people hungry for censored information and desperate to have their voice heard speed is probably not the biggest worry.

These networks are also frequently used by multinational corporations to connect networks across national boundaries, sometimes leaving a kind of backdoor for employees of a company in, say, China, to access a network hosted in another country with less restrictions. However, China has been targeting VPNs. Last year the Chinese government started monitoring and restricting traffic over routers connecting to foreign networks to better prevent misuse of VPNs. (http://www.guardian.co.uk/technology/2011/may/13/china-cracks-down-on-vpn-use).

Popular commercial VPN services include Tunnelbear (http://www.tunnelbear.com) and Strong (http://strongvpn.com/) but these may be inaccessible from within strongly filtered web infrastructures; China has preemptively prevented Tunnelbear from working inside China, for example. Strong VPN offers a free version called Open VPN, and according to their website:

Usually Open VPN will work in places where PPTP VPN is blocked. Places we have seen PPTP VPN blocked are locations in the Middle East like Oman, Dubai and UAE. That's not to say our PPTP VPN accounts won't work there, some customers report no problems. It depends on your ISP usually, and your local network. (http://strongvpn.com/compare.shtml)

These tools are just a couple of the resources available to help open access beyond closed borders on the Internet, and hopefully protect the identities of their users in the process.

The information above is all found on the Internet. I could get it freely, with no worries about governmental blocking or visits by secret police in the middle of the night. I can criticize my government, I can demand improvements in human rights, and I can do it without trying to hide. Someday, I hope the same can be true for all.

For more information about issues of freedom of speech and the open Internet, I highly recommend you visit the Electronic Frontier Foundation website at https://www.eff.org/ and the OpenNet Initiative at http://opennet.net/. These organizations are at the forefront of the fight for an open Internet for all. Reporters Without Borders is another very important organization, which focuses on freedom of speech both on the net and off. See them at: http://en.rsf.org/.

Data Security

Of course, issues of freedom on the Internet call for more than anonymity of access and bypassing blocks; securing your data at home and on the net is an ongoing struggle for everyone. Data security is possibly one of the most important issues of the 21st century. It affects everyone, from consumers shopping at home to governments planning wars. Of course, when you are a political dissident under an oppressive regime, keeping sensitive information safe from prying eyes is vital.

So now let's look at different ways of encrypting and securing your data in the wild.

Email Encryption

You should always realize, when you send any information over the Internet there is a chance someone could intercept it. Commercial websites almost universally use some form of TLS or SSL encryption to protect malicious interception of your personal data, but this is not usually the case for emails. Thus, if you are sending sensitive or even mildly personal data through your email, it's up to you to protect it. Luckily, there are several ways you can do that.

One of the oldest applications of public source, freely available encryption software is PGP, or Pretty Good Privacy, Encryption. Established by Philip Zimmerman (http://www.philzimmermann.com/EN/background/index.html) in 2002, but using work began in 1991, the PGP Corporation is now part of Symantec (http://www.symantec.com/theme.jsp?themeid=pgp). Unfortunately, this means it's now a paid service, but it offers an extremely robust and deeply comprehensive encryption suite that not only offers email protection, but can encrypt all your files and indeed your whole hard drive. It's not cheap, but it is secure.

Free services do exist, and they offer specific security solutions for private users of all kinds. For Gmail users, there are a couple of useful applications. One, encipher.it, has been profiled on Makeuseof.com here: http://www.makeuseof.com/tag/encrypt-gmail-facebook-messages/, and another that seems promising is a Greasemonkey script called, simply, Gmail Encrypt. http://www.langenhoven.com/code/emailencrypt/gmailencrypt.php. Of course, there are solutions that aren't specific to one email service, and you can find a good look at a few of them here: http://www.makeuseof.com/tag/ways-easily-quickly-encrypt-files-emailing/.

One important thing to remember about email encryption, though, is that it adds one more layer of effort to your email

access. Both the sender and receiver must have the same encryption keys, otherwise your emails and files will just be gibberish, so you will have to coordinate closely at both ends.

Disk & File Protection

The data you send over the Internet is far and away more vulnerable than the data on your hard drive, but even so there is a risk of unauthorized access. Naturally, in these increasingly mobile times, we carry our data with us in all kinds of formats: laptops, flash drives, SD cards, and on and on…and all of these can (and do) get lost frequently.

In the unlikely case that you lose a flash drive containing truly sensitive data, knowing that you took the extra step of encrypting that data should reduce your regret a bit.

Just like email encryption, there are a number of software suites that offer security at the file or disk level, and in fact some of the same software used for email protection can do the same for the files on your hard drive. The aforementioned PGP Encryption from Symantec offers this and more, but again for a price.

So let's look at some free options.

One highly recommended solution is Truecrypt: http://www.truecrypt.org/. It's an open source suite for Windows, Linux and Mac OS with on-the-fly encryption, making it free, convenient and highly useful. For a more detailed description and review, Makeuseof.com has a good article here: http://www.makeuseof.com/tag/encrypt-your-usb-stick-with-truecrypt-60/. Truecrypt is robust enough that the FBI was unable to crack it with a year to try, which I assume should be enough to protect you from all but the most highly skilled and well equipped hackers.

Another program, called CrossCrypt, allows you to create an "encryption drive" on your Windows computer so that encryption is simply a matter of saving to that drive. Again, it's open source and free to use, and offers a robust level of encryption, up to /aes256 bit encryption. It can be found here: http://www.scherrer.cc/crypt/

Plus of course, both of the major OSs, Mac and Windows, offer full disk encryption out of the box for some users. Mac's FileVault and Windows BitCrypt both use 128-Bit AES full disk encryption, although Microsoft only includes the software for Ultimate and Enterprise editions of Vista and Windows 7. These are really only useful for protecting the data on your box rather than files you're taking on the road, but they're strong and if your computer is physically compromised (stolen or lost) then your data should still be safe.

There are any number of other data encryption suites, and there is simply no way to give an overview of all of them. For those wanting to compare the available options, I highly recommend this comparison on Wikipedia: http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software .

2. International Netting Practicalities

Having dealt with the heavier issues of the Internet as a truly worldwide phenomenon, let's look at some of the less pressing, but perhaps more common, elements of international netting. I'll look at specific information that should be of use for travelers, expats, and more. We'll discuss how to find Internet access abroad, how to deal with language issues, and how to use some of the tools we discussed earlier to get your favorite entertainment regardless of your geographic location.

For The Traveler

Let's start by examining issues affecting the traveler abroad. Whether you're a backpacker lugging your iPad around the train stations of Europe, or a business traveler stuck in a hotel in Singapore, here's what you need to know to check your mail, Skype with your friends, and more.

Finding Access

The Internet is everywhere, for limited values of everywhere. Any major city you visit, almost anywhere in the world, will have some kind of Internet access. As I mentioned in the last chapter: even Pyongyang has an Internet café now! The question, though, is how much you have to pay and how to find it.

It is important to remember that patterns you might have in North America or Britain might not hold true in other countries. In the US, for example, coffee shops offer Wi-Fi, usually for free. But in Japan or Shanghai? Not so much. Conversely, train stations in the States aren't really a place where people hang out to check their email, but in Germany you could very well find a free hotspot right in the Hauptbahnhof.

Net Cafés & The Backpacker

For the student traveler, Internet cafes can be a life saver. They are nearly ubiquitous (more so in the West than the East, it must be said. There seems to be one on every street corner in Berlin or Paris, but barely a handful in Hiroshima). Net cafes run the gamut from slick corporate establishments to hip modern spots to shady back alley setups full of WOW kids. Prices, of course, follow that pattern. A good tip is, the grungier the mousepad, the cheaper the rates.

When traveling in Europe, I found that the most reliable, easily accessible and reasonably priced net cafes was Easy-Internet (http://en.wikipedia.org/wiki/EasyInternetcafé). The rates were decent, and most importantly they usually had a place to get coffee attached. Of course, there are lots of others to try, but it is important to remember a few points of etiquette that may differ from place to place.

When I was a student in St. Petersburg, the Internet cafes always required a drink order - the "café" was meant literally. A similar pattern holds true in many Internet cafes in Japan. It's always a good idea to check for purchase requirements like that before you go in.

Other requirements are a bit more onerous. As mentioned above, Italian Internet cafes require all users to submit their passports for copying. No passport, no Internet. In China, real name registration with ID might also be required. So if you're worried about providing your personal ID in some shady Internet dive, it might be a good idea to give net cafes in these countries a pass.

Using Hotels, Hostels etc.

If you are carrying your own net-enabled device, you can often get access through businesses you use. For backpackers, hostels often provide free or very cheap Internet access. Obviously, speeds might be low and security might be

lacking, but for occasionally checking your email it certainly does the trick.

Hotels often offer the same service, but remember that the higher the hotel rates, the higher the net prices as well. In higher end hotels, it can get really, really expensive. Again, check before you use. An important note: even at very good hotels in Asia, even in Japan, there is often no wireless Internet, it's only wired. If you're carrying an iPad you might be out of luck. In the Philippines, there are apparently restaurants that offer Wi-Fi for their patrons, as well, but you often have to pay.

The Holy Grail: Free Wi-Fi

The true budget traveler, of course, is always looking for free Wi-Fi. It is rare outside North America, but it does exist. When I lived in Berlin I would often make the trek to the Sony Center at Potsdamer Platz to take advantage of their public hotspot. It was limited to 90 minutes, but all you had to do was log in under a new name to continue…well worth the trip! So if you look around, it can be found.

Online Sites

The first place to check when you're on the hunt for free Wi-Fi is online. http://www.wififreespot.com/ is a great first step. It's a database compiled by users and travelers of public hotspots. It's widespread, but there are gaps.

For European information try http://www.free-hotspot.com/index.php?lang=en , a group that actually offers free Wi-Fi across the continent. Their offerings seem focused on fast food places and hotels, which are pretty widespread everywhere.

For information specific to the US or Japan, try: http://freewifispots.net/

Of course a little Googling can help you find more, but these are great places to start. One thing to keep in mind is that these are all listings of public spots, freely available. There are those who open their personal Wi-Fi, whether by accident or design. To find those, all you need is a Wi-Fi enabled device scanning for open networks. Just remember, those are unsecured and provided by the generosity of others. Don't abuse them, and don't be stupid.

Likely Locations

When you're travelling, and haven't done your research, there are a few spots you can try that are likely to offer free Wi-Fi. First, travel hubs are a good bet. Train stations in Europe, airports pretty much anywhere, etc. They all often have a variety of networks, paid and free, for travelers. Again, you'll need a device scanning for networks.

Other places to check are tourist spots with seating. The aforementioned Sony Center at Potsdamer Platz in Berlin is a good example. In Rome, there are some hotspots in larger piazzas. It can't hurt to check anywhere where there are lots of people not moving.

Security

It really should go without saying, but you must remember - on the road, you are at the mercy of the net provider you're using. And of course, don't forget the high possibility of usage monitoring at net cafes/public hotspots. It's vital that you be careful with your personal data.

When you're using a public computer, like at a net café, you should always avoid doing anything sensitive - logging into bank accounts, sending credit card details, using PayPal. Anything you wouldn't trust with a stranger, you shouldn't trust to a net café. Also, ALWAYS LOG OUT.

Dropbox, email, Facebook: whatever you log in to, always be careful to log out before you leave the computer, as well as unchecking those little "remember me on this computer" boxes. Logging into public Wi-Fi is perhaps a little safer, as you are using your own device, but there are still real risks. It is impossible to be too careful here, and the consequences for your privacy could be serious for a pretty small lapse in attention.

However, if you absolutely must access personal information, a little preparation is in order. For example, some private net cafes (as opposed to major chains like EasyInternet) allow you to use USB drives, meaning you can get a live USB stick with your own clean operating system running on their computer. It only bypasses software exploits or keyloggers, but it's a big step up in security.

There are several Linux systems that work from a USB, and even Windows 8 will be workable off a USB drive. When running your OS from the USB, try using an on-screen keyboard that allows you to input characters with mouse clicks rather than keystrokes, to foil hardware-based keyloggers. But really, just use your head, think in advance and do your best to avoid this kind of risk.

3. Special Notes For The Expat

The issues faced by travelers are a bit different from those of the expat: if you are living and working in another country, you probably have Internet access. However, expats face their own set of problems, and that's what's outlined in this third chapter.

Setting Up a PC While Abroad

If you go into another country without your own computer, or live in another country long enough for your computer to become obsolete, you will probably end up buying one. Computers are, luckily, pretty much the same anywhere. Windows is Windows, whatever the language, and Apple's OS X is universal too.

One major problem that people run into, however, is language. Living abroad, you may be amazed to find that English is not the default language for everything everywhere. Who knew? Apple seems to allow users to freely select their system language, but the same is not true for computers running Windows.

When you are buying a computer in another country, you need to figure out if you can get by in the local language or not. If you fall into the former group, then the world is your oyster and you can skip ahead. If, however, you like knowing what those big red error boxes actually say, you might want to find out if you can get an OS in your native language. My personal experience is that major retailers and makers do offer an English OS if asked, but as it is a special order, be prepared for extra time and expense.

Also remember that if you get an English OS there can be problems if you try to install software in another language, particularly if that language uses special characters. Those characters may not be enabled in your English language OS, meaning they'll just be nonsensical gibberish on your screen. This is especially problematic with languages which use no Roman characters at all, like Chinese, Japanese, or Russian. If you plan on using such software, it might be worth considering using the native OS.

There are a couple of other options besides specially requesting an English OS for your new computer. For Windows 7, one easy solution is to purchase/upgrade to the Ultimate edition. It includes the capability to change the system at will, though it will cost you. Another, slightly less legitimate, solution is a program called "Vistalizator." This software allows you to download and install Microsoft's language packs for any version of Windows from Vista on.

There are a couple of problems: it doesn't always install total conversion, leaving some gaps (for example, Help files might not be converted over, meaning they're unavailable in the newly installed language). This software also breaks the Windows TOS, meaning you could be voiding your warranty and customer support from Microsoft. If you're willing to take the chance, however, it's free and it works like a charm. Or so I've heard.

One final issue that really causes headaches for expats (or the ones I talk to, at least) is a symptom of the growing cleverness of the net itself: automatic location detection. It seems that every major site owner, from Google to Amazon, is able to tell what part of the world you're accessing from. While this can be a great convenience if, for example, you're looking for local weather information, it can be a real pain if you're trying to read English language news when you're in another country.

Some sites — Amazon for example— allow you to choose your location or change the display language with a simple drop-down menu.

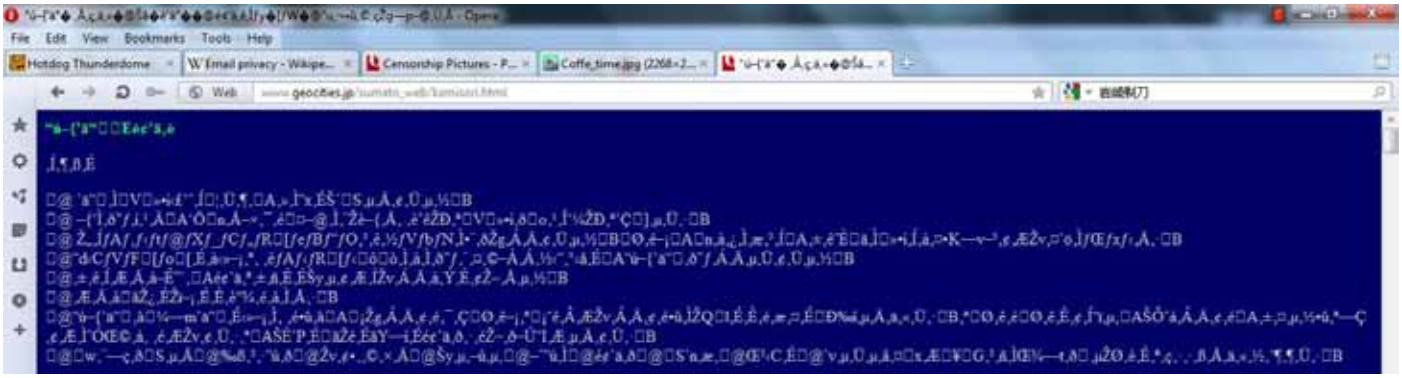
For others, especially Google services like Maps or Plus, you have to go into your account settings and make sure that your language is set to one you can read — which, if you can't read what's on the screen, could be really difficult. It helps if you are familiar with the general layout of the settings, but you might need to ask someone with the requisite language skills for help.

General Language Issues On The Net

Language is not only an issue for expatriates, of course. For those of us with an interest in the world beyond our own national borders, it can sometimes be difficult to find what we're looking for in a format we can understand. There are a lot of languages in the world, and no one can know all of them. Translation software can help with that, but before we get to that step there's something else we need to think about.

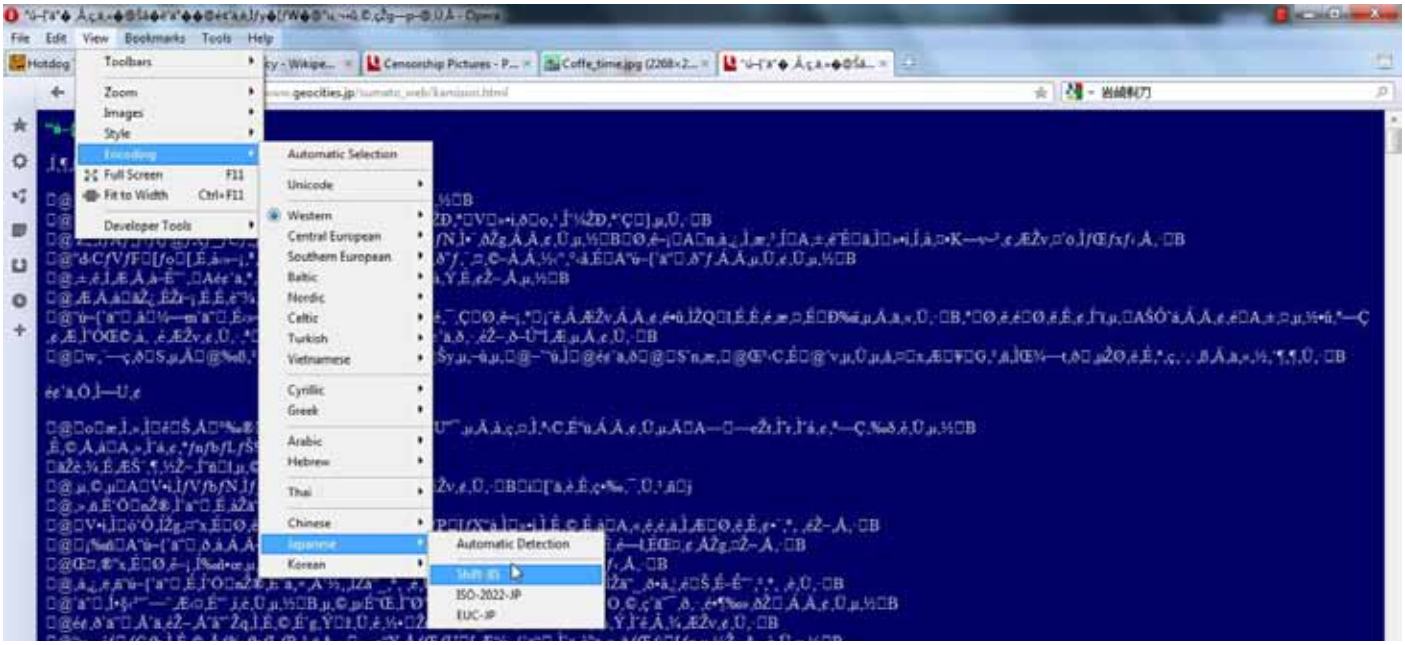
Displaying Non-Alphabetic Languages

Languages that use non-alphabetic writing, like Chinese characters, Cyrillic or Hindi, sometimes require special decoding for display on computers that don't natively support them. For example, people using American computers to access a Japanese page might very well see something like this:



The same can be true of any number of languages. What to do?

Well, if your computer has the language fonts installed, you can select how they are displayed in your browser. Go to the "View" menu on your browser, then select "Encoding." You'll see a drop-down list of all the various languages that your browser can display. Under each language, there can be several different encoding styles. You need to select the one that matches how this particular page was written, and the only way to do that is trial and error. For Japanese, and this page in particular, this is usually "Shift JIS," but for other languages I can't really say.



It's important to note here, the above does not really work for your iDevice. Safari for your iPhone or iPad does not allow that kind of manipulation, so you can't change the encoding from within your browser. One good workaround for this is the free app "Character Encoding Web Utility for iPad" (http://itunes.apple.com/jp/app/character-encoding-web-utility/id385731370), which allows just that. I use it, and find it extremely helpful.

Translation Tools & How To Get The Most Out Of Them

Once you are able to actually view the page you've accessed, you can decide if you're able to read it or not. Of course, if you can't, then you'll almost certainly turn to one of the many machine translation services on the Internet. Google Translate, BabelFish and many others are out there, some are better than others, but all have their limits. Plainly stated - machine translation like this is still extremely weak, and using them can be difficult to get more than a general idea of what a page is trying to say. That being said, there are a few tips that can help you.

First, try to break the page down into smaller sections. Instead of just plugging the URL into Google translate and letting it do the whole page, try copy-pasting a few words or phrases. When you have an idea of the words being used, try translating some complete sentences to get a grasp of the grammar. You will probably start to understand what you're reading more with some repetition. It's still not perfect, but it helps.

Another thing you can try is, instead of using a straight up translator is using a "text glosser," like the one at Jim Breen's WWWJDIC (http://mygengo.com/wwwjdic/cgi-data/wwwjdic?1C). These break a text down into smaller pieces and give you a word-by-word translation, like a dictionary would, along with an explanation of some grammar points, allowing you to put the pieces together yourself. It's more work, but you're more likely to get some sense out of the text that way.

This kind of focused work is probably most suited to language learners, but if you're really interested in learning about the world it could well be worth the effort. You might be surprised by what you're missing out on.

4. Accessing Region-Blocked Media

One unfortunate development on the net is the corporate establishment of artificial restrictions on content. The Internet itself is international, the information it carries recognizes no borders. But media producers like television stations and movie studios, are dead set on making their own.

This is, of course, their legal right, and that isn't going to change anytime soon. However, at the same time, it is a real pain for those of us wanting to watch the Daily Show outside of the US. There are ways to do that, of course, and we'll look at those for a bit.

Region Locking & What It Means For You

There are a growing number of online media streaming sites, many offered for free. This means that users can, for the most part, see or hear what they want, when they want it. Indeed, not only is this kind of distribution growing more common, it's reaching every device with net access. Smartphones, tablets, game consoles and more — they're all streaming enabled these days. That kind of convenience is appealing for everyone, of course, but the artificial blocks installed by distributors (at the undoubted request of copyright holders) can prevent access for a lot of people without the good fortune to be living in a random geographical location designated by a corporation as "acceptable."

With all that content out there waiting for an audience, a lot of people have found ways around the location blocking on their favorite streaming and download sites. Some of them will be familiar if you have read the rest of this manual.

VPNs, Tunneling & IPN Spoofing

The most straightforward way to gain access to region-locked content is to trick the site into thinking you're in the right place. VPNs and Tunneling services are simple ways to do this. At this point, an expat hungry for the latest Doctor Who episode intersects with a blogger hiding her identity from the Iranian secret police.

Free Services

There are any number of free VPN and tunneling services. Most of them have some limitations on usage, but they are still usable.

- *Tunnelbear (http://www.tunnelbear.com/) is a great new service that allows 500MB of usage a month for free, with a campaign adding another gigabyte if you tweet about their service. They've also added an iPad/iPhone app, allowing you to access blocked content on the go. If you're willing to pay, you can remove your usage limits completely. It's also easy to use, with a simple "on/off" interface and the option of choosing your location - UK or the USA, depending on what content you want to access.*

- *PrivateTunnel (http://www.privatetunnel.com/) offers 100MB of free access a month. It's a bit more complex than Tunnelbear and includes some security options that might be more strict than what you want, but it is fast and reliable.*

- *Hotspot Shield (http://hotspotshield.com/) is a security/VPN service that not only allows you to tunnel into US or UK based servers for content access, but also increases your security against malware and adds HTTPS protocols to your browsing to help protect your personal information.*

There are many more services like this, but these are probably the three biggest and most popular.

Paid Services

All of the services above also include paid versions, increasing your usage caps or improving service in general. There are also services which don't offer free versions, and the main difference is they tend to offer a bit faster, smoother connections with better customer service.

StrongVPN (http://www.strongvpn.com/) is one of the biggest, most popular VPN services on the net. They offer tunneling to 19 different countries, with higher speeds and better connections than the free services above. They have several price levels, the cheapest starting at US$7 a month, so if your budget can afford that much, it might well be worth it for the added peace of mind.

HideIPVPN (http://www.hideipvpn.com/premium_vpn/) is another free/premium service but their "free version" is only a three hour trial. They have a slick interface, but their quality falls a bit behind StrongVPN, at least from Japan.

There are any number of other paid VPN services as well, but really, in terms of budget and reputation it looks like StrongVPN is the top of the heap.

These services tend to slow down connections a little, but generally you can stream video or audio with few problems-

Good luck!

The Final Word

I hope the information contained in this guide was at least interesting, if not helpful. The Internet is worthy of every effort to move beyond your borders. This guide was written to help people do that, and hopefully make the world a little smaller.

Image credits:

Page 5, Map or World is credited with "© Raimond Spekking / CC-BY-SA-3.0 (via Wikimedia Commons)" More information: http://commons.wikimedia.org/wiki/File:Daumenschellen_(Thumbcuffs_Bondage)_Model_Ina.jpg

Page 15, Padlock With Keys by Petr Kratochvil. More information: http://www.publicdomainpictures.net/view-image.php?image=2909&picture=padlock-with-keys

Did you like this PDF Guide? Then why not visit MakeUseOf.com for daily posts on cool websites, free software and internet tips?

If you want more great guides like this, why not subscribe to MakeUseOf and receive instant access to 50+ PDF Guides like this one covering wide range of topics. Moreover, you will be able to download free Cheat Sheets, Free Giveaways and other cool things.

Home:	**http://www.makeuseof.com**
MakeUseOf Directory:	**http://www.makeuseof.com/dir**
MakeUseOf Answers:	**http://www.makeuseof.com/answers**
Geeky Fun:	**http://www.makeuseof.com/tech-fun**
PDF Guides:	**http://www.makeuseof.com/pages/**
Tech Deals:	**http://www.makeuseof.com/pages/hot-tech-deals**

Follow MakeUseOf:

RSS Feed:	**http://feedproxy.google.com/Makeuseof**
Newsletter:	**http://www.makeuseof.com/join**
Facebook:	**http://www.facebook.com/makeuseof**
Twitter:	**http://www.twitter.com/Makeuseof**

Think you've got what it takes to write a manual for MakeUseOf.com? We're always willing to hear a pitch! Send your ideas to justinpot@makeuseof.com; you might earn up to $400.

Download Other MakeUseOf PDF Guides!

http://makeuseof.com/pages