```
jazzfrobot:~ $ open catfood
catfood: Unable to open catfood
Permission denied
jazzfrobot:~ $ cat > canopener.py
#!/usr/bin/python
import socket
sock = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
sock.connect(('127.0.0.1',7500);)
crash = '\x41'*1337
eip = '\xFF\xFE\xEF\x08'
payload = open("msf-bindshell-4444.bin").read()
sock.send(crash+eip+payload)
sock.close()
jazzfrobot:~ $ chmod +x canopener.py; ./canopener.py
jazzfrobot:~ $ nc -vv localhost 4444
localhost [127.0.0.1] 4444 (?) open
# open catfood
Opening delicious catfood...
```

Protecting Security Researchers' Rights in the Americas

ELECTRONIC FRONTIER FOUNDATION

Authors: Nate Cardozo, Kurt Opsahl, Katitza Rodríguez, Ramiro Ugarte, and Jamie Lee Williams

A publication of the Electronic Frontier Foundation, 2018.

View this report online: https://eff.org/coders-rights-americas

Protecting Security Researchers' Rights in the Americas

Nate Cardozo, EFF Senior Staff Attorney
Kurt Opsahl, EFF Deputy Executive Director and General Counsel
Katitza Rodríguez, EFF International Rights Director
Ramiro Ugarte, EFF consultant
Jamie Lee Williams, EFF Staff Attorney

With contributions from Tamir Israel, Staff Attorney, CIPPIC

SEPTEMBER 2018

Executive Summary

Computer security researchers work, often independently from large public and private institutions, to analyze, explore, and fix the vulnerabilities that are scattered across the digital landscape. While most of this work is conducted unobtrusively as consultants or as employees, sometimes their work is done in the public interest—which gathers researchers headlines and plaudits, but can also attract civil or criminal suits.

Sometimes they are praised for exposing dangerous flaws in computer software and the machinery that depends on it; on other occasions, corporations and governments scramble to use the law to silence and punish what they see as dangerous pronouncements, including the revelations of these flaws to the general public, and demonstrations of how the flaws might be exploited.

Security researchers who attempt to improve infrastructure are targeted and threatened with laws intended to prevent malicious intrusion, even when their own work is anything but malicious. The result is that security researchers work in an environment of legal uncertainty, even as their job becomes more vital to the orderly functioning of society.

What rights do security researchers have? How are those rights expressed in the Americas' unique arrangement of human rights documents and institutions? And how might we best interpret the requirements of human rights law, including rights of privacy, free expression, and due process, when applied to the domain of computer security research and its practitioners?

Drawing on rights recognized by the American Convention on Human Rights, and examples from North and South American jurisprudence, EFF is introducing a Coders' Rights project to connect the work of security research with the fundamental rights of its practitioners. Through this project we will support the right of free expression that lies at the heart of researchers' creation and use of computer code to examine computer systems and relay their discoveries among their peers and to the wider public; the importance of establishing intent in laws surrounding computer intrusion; the dangers of "terms of service" of private entities to create criminal liability among researchers by redefining "unauthorized access"; and the obligation of legal systems to provide punishment proportionate to the crime, especially when cybercrimes demonstrate little harmful effects, or are comparable to minor traditional infractions.

The goal of this project is to promote standards that lawmakers, judges, and most particularly the Inter-American Commission on Human Rights might use to protect the fundamental rights of security researchers, as well as ensure the safe and secure development of the Internet and digital technology in the Americas and across the world.

To that end, we will argue that the courts and the law should guarantee that the creation, possession or distribution of tools related to cybersecurity are protected by

Article 13 of the American Convention of Human Rights, as legitimate acts of free expression. We will call on lawmakers and judges to discourage the use of criminal law as a response to socially beneficial behavior by security researchers. We will demand that cybercrime law include malicious intent and actual damage in its definition of criminal liability, and that penalties for computer crimes be proportionate to the harm caused, and match comparable crimes conducted without the use of a computer. Finally, we will call for proactive actions that would secure the free flow of information in the security research community.

Code is Expression: Computer Programming as Expressive Activity Protected by the American Convention of Human Rights

Before turning to a description of various restrictions on security researchers' rights, we begin with an overview of the right to freedom of expression as it is protected in the Inter-American system, and show why this right extends to protect security researchers. In particular, we will explain why freedom of expression applies to the computer code that is frequently used to convey meaning between security researchers, their clients, and the general public.

Article 13 of the American Convention, which guarantees the right to freedom of expression, provides:

1. Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.
2. The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure: a. respect for the rights or reputations of others; or b. the protection of national security, public order, or public health or morals.
3. The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.
4. Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.
5. Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action

> against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.

The Inter-American Court of Human Rights (IA Court) and the Inter-American Commission of Human Rights (IACHR) have recognized that the right to freedom of expression is instrumental to democratic institutions. The IACHR has stated that "[t]he legal framework of the Inter-American system for the protection of human rights is probably the international framework that provides the greatest scope and the broadest guarantees of protection to the right to freedom of thought and expression."[1] The IACHR explains:

> From a comparative perspective, when the texts of Article 13 of the American Convention, Article IV of the American Declaration, and Article 4 of the Inter-American Democratic Charter are contrasted with the relevant provisions of other international human rights treaties–specifically with Article 19 of the International Covenant on Civil and Political Rights or with Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms—it is clear that the Inter-American framework was designed by the American States to be more generous and to reduce to a minimum the restrictions to the free circulation of information, opinions and ideas.[2]

This broad protection of freedom of expression is linked, in the Inter-American system, to the functions this right performs in a democratic society and to its relationships to the human capacity to create and innovate. Focusing on creativity and innovation, the IACHR has asserted that:

> … it is one of the individual rights that most clearly reflects the virtue that marks – and characterizes – human beings: the unique and precious capacity to think about the world from our own perspective and communicate with one another in order to construct, through a deliberative process, not only the model of life that each one has a right to adopt, but the model of society in which we want to live. All our creative potential in arts, in science, in technology, in politics—in short, all our individual and collective creative capacity—fundamentally depends on the respect and promotion of the right to freedom of expression, in all its dimensions. This is therefore an individual right without which the first and foremost of our liberties would be denied: our right to think by ourselves and share our thoughts with others.[3]

While the standards developed by the Inter-American system of human rights protect all sorts of speech, the special relationship between speech and the functioning of democratic institutions, and between expression and human creativity and innovation,

[1] CIDH, Marco Jurídico Interamericano Del Derecho a La Libertad de Expresión (Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, 2010), par. 3.
[2] *Id.*, par. 3.
[3] *Id.*, par. 7.

distinguish *certain* kinds of speech as specially protected. Free expression encompasses not only the right to impart information, but also to seek and receive it. In that sense, the reasoning of the bodies of the Inter-American system of human rights is essential to protecting researchers' rights, and establishing that *code* is protected by Article 13 of the American Convention of Human Rights.

This argument has been developed in the United States based upon the First Amendment to its Constitution. Key judicial decisions in the United States have recognized the expressive nature of code. In the landmark decision *Bernstein v. United States*,[4] the court found that code is protected by the First Amendment, as a form of conveying meaning and exchanging information. This has been affirmed by courts in the United States in other cases.[5]

In Latin America, the argument is even stronger because the rich and nuanced text of Article 13 of the American Convention lends itself more easily to defending freedom of expression when carried out in computer code. In that sense, Article 13 provides a textual basis for an argument that—in the case of the First Amendment—has been developed out of the principles it stands for.

Coding is a form of expressing ideas in what is usually known as *high-level* languages. These languages are meant primarily to instruct computers, usually to the benefit of some human endeavor. There are many computer languages, and coders usually know more than one. These languages operate with their own rules of grammar and syntax, and code written in them is primarily meant to be read by humans. As explained in *Bernstein*:

> A computer, in fact, can make no direct use of source code until it has been translated ('compiled') into a 'low-level' or 'machine' language, resulting in computer-executable 'object code.' That source code is meant for human eyes and understanding, however, does not mean that an untutored layperson can understand it. Because source code is destined for the maw of an automated, ruthlessly literal translator—the compiler—a programmer must follow stringent grammatical, syntactical, formatting, and punctuation conventions. As a result, only those trained in programming can easily understand source code.[6]

Code is a way of expressing ideas in a precise and clear fashion. As EFF argued in the context of the *Bernstein* decision,

[4] *Bernstein v. United States Department of Justice*, 922 F. Supp. 1426 (1999).

[5] *See*, e.g., *Universal City Studios v. Corley*, 429 F.3d 445 (2000). (arguing that "[c]ommunication does not lose constitutional protection as 'speech'" simply because it is expressed in the language of computer code") and *Junger v. Daley*, 481 F.3d 484 (2000). (arguing that "[t]he First Amendment protects code because, like a musical score, it 'is an expressive means for the exchange of information and ideas.'").

[6] *Bernstein v. United States Department of Justice*, 922 F. Supp. 1426, 4230 (1999).

> "[j]ust as everyday thoughts are expressed in natural language, and formal deductions are expressed in mathematical language, methodological thoughts are expressed in programming languages. A programming language is a medium for communicating methods, not just a means for getting a computer to perform operations—programs are written for people to read as much as they are written for machines to execute."[7]

In that sense, expressing algorithms in a computer language increases precision of communication. In the words of the pioneering computer scientist Donald Knuth in his definitive work on algorithms, *The Art of Computer Programming*:

> Each step of an algorithm must be precisely defined; the actions to be carried out must be rigorously and unambiguously specified for each case. The algorithms of this book will hopefully meet this criterion, but since they are specified in the English language, there is a possibility the reader might not understand exactly what the author intended. To get around this difficulty, formally defined 'programming languages' or 'computer languages' are designed for specifying algorithms, in which every statement has a very definite meaning. Many of the algorithms in this book will be given both in English and in a computer language. [8]

The U.S. Court of Appeals for the Second Circuit in the case of *Universal City Studios v. Eric Corley* has also stated that programming languages and code, for certain fields of human knowledge, are the preferred language for expressing ideas and conveying meaning:

> Communication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code. Mathematical formulae and musical scores are written in 'code,' i.e., symbolic notations not comprehensible to the uninitiated, and yet both are covered by the First Amendment. If someone chose to write a novel entirely in computer object code by using strings of 1's and 0's for each letter of each word, the resulting work would be no different for constitutional purposes than if it had been written in English. The 'object code' version would be incomprehensible to readers outside the programming community (and tedious to read even for most within the community), but it would be no more incomprehensible than a work written in Sanskrit for those unversed in that language. The undisputed evidence reveals that even pure object code can be, and often is, read and understood by experienced programmers. And source code (in any of its various levels of complexity) can be read by many more. Ultimately, however, the ease with which a work is comprehended is irrelevant to the constitutional inquiry. If computer code is distinguishable from conventional speech for First Amendment purposes, it is not because it is written in an obscure language.[9]

[7] EFF, *Brief in the Case of Bernstein v. United States Department of Justice* (1996).

[8] Donald E. Knuth, *The Art of Computer Programming*, Vol. 1: Fundamental Algorithms, (3 edition ed. 1997).

[9] *Universal City Studios v. Corley*, 429 F.3d 445, 445–446 (2000).

From this perspective, code plays a fundamental role in modern society. While we do not usually see it, computer code is all around us. Whole fields of human knowledge, now depend for their advancement on ideas expressed in computer code: not just computer science, but also branches of economics, statistics, chemistry and biology. New economies based on information thrive based on it. Technology companies often reach leading positions because they write better code than their competitors.

Alternatively, the free software movement is based on the idea of code transparency: anyone can read, write, and modify the computer code that is freely shared by the movement's participants. These conditions have created complete and functional operating systems—an example of complex communally-created works manufactured from acts of free expression.

Relevant to the particular context of security researchers, it is also notable that Article 13 protects the right to seek and receive information. This right can be engaged robustly where the information sought is critical to public governance or safety. Therefore, the prohibitions on accessing information critical to the security and integrity of important networks should also fall under the weight of Article 13's high standards of protection.

It makes sense, then, to analyze the text of Article 13 in order to understand how code fits into its language:

> "**information and ideas of all kinds**" – This guarantee implies that those states which have signed the Convention cannot use distinctions between the types of ideas which are being distributed to determine whether they are the result of human creativity. Ideological differences, modes of expression (press, cinema, photography, and so on), and kind of information (political, cultural, scientific, and so on) must be treated in a neutral manner by the state. It is not possible to identify certain ideas in order to prohibit them, except for the ones expressly included in Article 13.5.
>
> "**in writing**" – Article 13 expressly guarantees the dissemination of ideas in writing, which is how ideas expressed in code are distributed. Programming languages are written languages, which may—or may not—be executed by computers. These languages follow logical parameters, respect rules of syntax, and have grammatical structures pre-defined.
>
> "**... or through any other medium of one's choice.**" – Article 13 of the American Convention reflects the development of the multiple expressive mechanisms developed until 1969. Radio, television, cinema—these are forms of expression the writers of the U.S. First Amendment could not imagine in 1791. However, they were part of the daily routine of millions of humans as of 1969. These days, to that catalog of expressive mediums we must add Internet-based communications, which are made possible by a handful of computer languages (CSS, HTML5, and JavaScript, among others) that make the transmission of ideas in human language possible within a broad, decentralized computer network.

Code is, then, a way of expressing ideas and conveying meaning. Furthermore, it is an essential form of expression or a field of knowledge that has become essential for the well-being of democratic societies: that of security research. Indeed, security researchers engage in an ongoing dialogue aimed at keeping the Internet a free, open, and secure space.

Cybercrime and Free Expression in the Americas

In this section, we examine various formulations of cybercrime offenses and assess these against the expressive rights of security research.

It could be argued that some interference with free expression is permitted and justified when it comes to malicious, socially undesirable behavior. However, as explored below, some criminal laws are too vague and broad regarding what constitutes criminal acts, and may indeed constitute a disproportionate encroachment into users' free expression and the freedom to innovate and compete in the economic market. We conclude that some formulations of the 'intent' requirement can provide a measure of protection for security researchers' expressive rights, and are therefore preferable.

A survey of Latin American regimes shows that the expressive dimension of code has not been directly addressed by legislators. A 2013 study shows a region active in the regulation of cyber-offenses and focused on the issues covered by the Budapest Convention: illegal access, interception, data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud.[10]

However, none of these offenses explicitly consider the potential effect these crimes can have on freedom of expression, a task that will have to be addressed by judges before any substantial restriction on this right. If so, they would have to apply the *three-prong* test the Inter-American system uses to balance restrictions: (a) it should be established by law; (b) it should be aimed at fulfilling a compelling state interest; and (c) it should be necessary in a democratic society.[11]

When it comes to cyber-criminal offenses, the right to free expression is implicated where cybercrime laws seek to punish the act of writing or sharing code in particular, and to a lesser degree when security researchers seek to obtain information exposing security flaws. But cyber-offenses in the region fail to account for this, where the main bulwark against abuse lies in the scope of the offense and the intent requirement.

[10] Marcelo Gabriel Ignacio Temperini, *Delitos Informáticos En Latinoamérica: Un Estudio de Derecho Comparado. 1ra. Parte.* in 1er. Ccongreso nacional de ingeniería informática/sistemas de información (2013), *available at* http://conaiisi.unsl.edu.ar/ingles/2013/82-553-1-DR.pdf.

[11] CIDH, *Marco Jurídico Interamericano Del Derecho a La Libertad de Expresión*, III.68.

The scope of activity expressly prohibited by cyber-offense legislation can include any unauthorized access to a given computing system or network, or it can be limited to intrusive acts which cause varying degrees of harm.

Similarly, the intent requirement, which is contained in each provision of the Cybercrime Convention and should "be taken into consideration when officials decide how to charge a crime,"[12] can be interpreted broadly or limited in scope with regard to more harmful intrusive activities. The intent requirement can provide some level of protection for security researchers, depending on how each internal provision is interpreted.

Prohibitions on Security Software

Security tools that could crack a system are also vital for testing computer and network security (with authorization from the target but simulating an attack without authorization) in order to detect security flaws often called penetration testing or "pen testing." Thus, the creation, possession, or distribution of security tools should not be criminalized, because such programs are not inherently bad. Rather, they can be used for both good and bad purposes.

However, the prohibition on communicating or selling computers or computer programs with the intent of allowing the access is sufficiently ambiguous to undermine legitimate activities needed for independent security research, academic study, and other good-faith activities that ultimately make the public safer.

Examples of software written exclusively to pen test include password-cracking programs such as Crack and John the Ripper.[13] System administrators often use these

[12] 9th Plenary of the T-CY, T-CY *Guidance Note No. 7. New Forms of Malware*, 4 (2013).

[13] See, e.g., Robert Morris and Ken Thompson, Password Security: a Case History, Commun. ACM, 22(11):594–597, 1979; Joseph A. Cazier and B. Dawn Medlin, Password Security: An Empirical Investigation into E-Commerce Passwords and Their Crack Times, Information Systems Security, 15(6):45–55, 2006; David C. Feldmeier and Philip R. Karn, UNIX Password Security -Ten Years Later, In CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, pages 44–63, London, UK, 1990; Daniel Klein, 'Foiling the Cracker': A Survey of, and Improvements to, Password Security, In Proceedings of the 2nd USENIX Security Workshop, pages 5–14, 1990; Arvind Narayanan and Vitaly Shmatikov, Fast Dictionary Attacks on Passwords Using Time-Space Tradeoff, In CCS '05: Proceedings of the 12th ACM conference on Computer and communications security, pages 364–372, New York, NY, USA, 2005; Philippe Oechslin, Making a Faster Cryptanalytic Time-Memory Trade-Off, Advances in Cryptology -CRYPTO 2003, 2003; Matt Weir et al., Password Cracking Using Probabilistic Context-Free Grammars, In SP '09: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy, pages 391–405, Washington, DC, USA, 2009; Aleksandar Kasabov and Jochem van Kerkwijk, Distributed GPU Password Cracking, System and Network Engineering research group, Informatics Institute, Faculty of Science, University of Amsterdam, 2011.

tools to determine when users have chosen insecure passwords that need to be changed. Academics and other researchers who are studying password security may also use them. Another classic example is Wireshark,[14] a "packet sniffer" (a program which intercepts and analyzes data passing across an ethernet or wireless network) which could be used for illegal wiretapping, but is primarily used by network administrators to debug network configuration problems or identify software bugs.

The development and use of these tools are necessary for research and testing, including for defensive security research to determine the feasibility of attacks on a system. Proofs of concept intended to display network vulnerabilities might be considered "computer programs," and thus their communication might fall within the prohibition as being done with the knowledge that the flaw might be exploited by malicious actors if not promptly fixed in time.

These interpretation dilemmas should be solved by judges considering the expressive dimension of code and the need to distinguish between expressive acts, which are part of the ongoing conversation in the field of cybersecurity, and actions that can produce harm and can be punished by the state. Furthermore, judges should also consider in their analysis the relationship between security research and the importance of keeping the Internet a free, open, and secure space.

Vulnerability Disclosure as Free Expression

As all knowledge-producing activities, security research depends on the free flow of information and the uninhibited exchange of ideas. A special subset of that research deals with the discovery, reporting, and solving of vulnerabilities in information systems. Just as important as discovering security flaws is reporting the findings so that users can protect themselves and vendors can repair their products.

For that reason, laws should also not criminalize the demonstration and disclosure of vulnerabilities. The criminalization of the act of demonstrating vulnerabilities gives vendors of flawed products the ability to deny the existence of flaws, even months or years after those flaws have been discovered, or to wrongly suggest that the vulnerabilities are merely theoretical. Criminalization also provides them with enhanced legal leverage to frighten researchers into silence. This harms the public by allowing insecure and broken technology to remain unpatched.

For example, in 2008 in the United States, the Massachusetts Bay Transit Authority (MBTA) sued three college students who were planning to give a presentation about vulnerabilities in Boston's subway fare system at a conference.

The MBTA improperly claimed that the students would violate the U.S. Computer Fraud and Abuse Act by delivering a talk to conference attendees that it claimed could be used to defraud the MBTA of transit fares. While a judge ultimately found that the

[14] Marcia Hofmann, 2011 in Review: Hacking Law, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2011/12/2011-review-hacking-law.

presentation would not have violated the law, the MBTA's baseless lawsuit initially prevented the students from presenting their research at the conference, infringing their free expression rights.[15]

At the 2010 Black Hat technical security conference in Las Vegas, professional security researcher Barnaby Jack publicly demonstrated that it was possible to bypass security measures on ATMs and program them to dispense money. Given the widespread use of ATMs by citizens and their legitimate concerns over the security of their accounts, there is a strong public interest in these kind of security flaws being known to the public, and vendors acting on information about vulnerabilities in a timely fashion as well as building machines and systems with the highest security standards possible. Jack was supposed to have given the talk at the conference the previous year, but his employer at the time, Juniper Networks, pressured him to cancel it after receiving a complaint from an ATM vendor. As a result, ATMs remained vulnerable for an entire year after Jack first intended to make their existence publicly known.[16]

These cases should inform the way criminal offenses are interpreted in the context of security research. For instance, Article 154 of the Brazilian Code permits an interpretation that would minimally impact the expressive acts engaged in by security researchers and such an interpretation should be favored.

Canada’s cybercrime regime includes a prohibition on the making, possession, or distribution of devices, software, or code where it can reasonably be inferred that the device in question has been or will be used to commit data mischief or unauthorized use of a computer service and has been primarily designed for that purpose.[17] The distribution offense is tied to data mischief and unauthorized use offenses and, as a result, courts should carry over the harm and fraudulence requirements built into the underlying offenses. However, the distribution provision itself carries no specific obligation to demonstrate intended harm or fraudulence, opening the door to a broad interpretation that would undermine the distribution and legitimate use of security.

Vulnerability reporting is part of a broader debate about the potential harms and benefits of publishing information that could be used maliciously. Vulnerability disclosures are unique in that they often include *proof of concept* code, a very specific way of explaining a security flaw to other coders and researchers.

Proof of concept code can be particularly problematic because it is both descriptive and functional and can be used or modified to create a program that will use the vulnerability to gain unauthorized access or otherwise interfere with the computer system.

[15] Electronic Frontier Foundation, *MBTA v. Anderson*, https://www.eff.org/cases/mbta-v-anderson.

[16] Kim Zetter, *ATM Vendor Halts Researcher's Talk on Vulnerability*, Wired.com, 2009, http://www.wired.com/threatlevel/2009/06/atm-vendor-halts-talk/; Kim Zetter, *Researcher Demonstrates ATM ‘Jackpotting’ at Black Hat Conferenc*e, Wired.com, 2010, http://www.wired.com/threatlevel/2010/07/atms-jackpotted

[17] Section 342.2.

Many security researchers have voluntarily adopted a delayed publication policy often called "responsible disclosure." While the details differ, the term has come to mean that the researcher discloses full information to the vendor, possibly discloses some information—but not proof of concept code—to the public, and refrains from publishing details that would allow an attacker to exploit the security flaw until the vendor issues a patch. In return, the vendor is supposed to expeditiously issue a fix and give credit to the researcher for his or her discovery.

Problems persist. Disclosure or the threat of disclosure often encourages quick patching, but when vendors do not act quickly to issue patches, the researcher may reasonably believe that the responsible thing to do is to disclose the problem so that customers can protect themselves. Vendors may have strong economic incentives to downplay or misrepresent risks, incentives that disclosure counteracts. Vendors may have contractual relationships with security firms that inhibit disclosure of important security information. Criminals disinterested in improving security may refuse to report security information to vendors or the public, so that the flaw will not be fixed and can be secretly exploited for economic or political gain.

This paper does not endorse any particular view of when disclosure is responsible. EFF believes that security researchers have a free expression right to report their research, including proof of concept code, and that disclosure is highly beneficial. However, it is a highly subjective question of when and how to hold back details to mitigate the risk that vulnerability information will be misused, so the law should only rarely police disclosures.

Criminal Intent and Security Research

Criminal laws should clarify the definition of *malicious intent* or *mens rea*, and avoid turning general behaviors into strict liability crimes. For example, in some cybercrime provisions the *intent* requirement is more clearly present in the way cyber-offenses are worded. Act 19.223 of Chile, for instance, punishes illicit access but establishes that, in order to be punishable, the action must be deployed with the intent (*desire*) of unlawfully getting, using, or learning information that is contained within a given information system. This subjective element safeguards the actions of researchers who might access systems with no permission but with no intention of causing harm. The same is established by Article 3 of Chile's act, which demands maliciousness to punish those who affect the integrity of data.

Canada's codification of the cybercrime convention similarly includes two complementary prohibitions. Those prohibitions are limited to the fraudulent use of a computing service (unauthorized use of a computer service), and acts that willfully and tangibly interfere with the use of data (data mischief).[18] The data mischief offense

[18] Criminal Code, RSC 1985, c C-46, Canada, section 342.1 (unauthorized use of a computer system) and sub-section 430(1.1)(mischief in relation to data), respectively.

provides a specifically itemized list of certain harms that must be willfully or knowingly caused by act or omission and are an integral component of the offense:

> Data Mischief s 430 (1.1) Everyone commits mischief who willfully (a) destroys or alters computer data; (b) renders computer data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of computer data; or (d) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it.[19]

An opposite, and problematic, solution is offered by Article 269A of the Colombian Criminal Code, which sanctions access without authorization whether there is a concrete damage or not.[20] Allowing security researchers to test a computer system without explicit permission is necessary for a vast amount of useful research, which might never be done if permission were required. Indeed, independent researchers have revealed so many security flaws to vendors that many vendors have set up a "bug bounty" program to explicitly encourage and reward this research.[21]

In a similar way, Article 196 of the Criminal Code of Costa Rica punishes whomever simply accesses a system without authorization.[22] Possibly the clearest example of the kind of problems that arise out of this approach is Article 202.1 of the Ecuador Criminal Code:

> He who employing any electronic media, computers, or similar, violates passwords or security systems, to access or obtain protected information, contained in an information system; to break the secret, confidentiality or

[19] Sub-sections 430(1.1) and 429(1), Criminal Code, Canada. Acts committed with legal justification or excuse or with colour of right are excluded (see sub-section 429(2)).

[20] Article 269 A of the Colombian Penal Code. Who, without authorization or otherwise agreed, access ePn all or part of a computer system protected or not with a security measure, or remain within it against the will of whoever has the legitimate right to exclude it 18 USC § 2702: Will incur a prison sentence of forty-eight (48) to ninety-six (96) months and in a fine of 100 to 1,000 legal minimum monthly salaries in force.

[21] See, for example, Russell Brandom, "*Facebook paid $15,000 to close a bug that could unlock any user's account*," The Verge, 8 March 2016, (https://www.theverge.com/2016/3/8/11179926/facebook-account-security-flaw-bug-bounty-payout)

[22] Article 196 of the Criminal Code of Costa Rica. Any person who, with danger or damage to the privacy or privacy of a third party, and without his / her authorization, diffuses or diverts from their destination documents or communications addressed to another person will be punished. The penalty will be four to eight years in prison if the described behaviors are carried out by: a) The persons in charge of the collection, delivery or safeguard of the documents or communications. B) The persons in charge of administering or giving support to the system or computer network or telematics, or that, due to their functions, have access to such system or network, or to electronic, optical or magnetic containers.

> reserve, *or simply to break security*, will be punished with a time in prison between six months and a year and a monetary penalty of 500,000 US dollars [emphasis added].[23]

Without a malicious intent requirement, this statute harshly criminalizes "breaking security," potentially without any requirement for harm or damage, and seemingly without regard to whether the purpose was beneficial.

These sorts of regulations can have a chilling effect on important security research. Consider a security researcher who has identified a vulnerability, but has not actually exploited it to gain access to a system. All too frequently, after the researcher discloses the problem to the vendor, the vendor will deny that it's a problem. The researcher may need to provide a proof-of-concept exploit to disprove the denial and convince the vendor to fix the problem. However, if the vendor can deny permission and is backed by these broad and harsh laws, the vendor may be able to hide the flaw, and the network will remain insecure.

These proof-of-concept reports are usually expressed in code and are functional or mostly functional.[24] Without clear legal definitions that allow experts to create or convey this code, legislation can chill not only research into vulnerabilities but also the steps needed to fix or ameliorate them. A provision such as Article 274G of the Criminal Code of Guatemala, for instance, does not distinguish between an academic or technical paper which describes vulnerabilities in order to denounce them from the actions of those who—using similar code—exploit these vulnerabilities to gain something out of it.[25]

Judges and Interpretations

Regulations that do not specify the need for volition or intent to constitute a crime do not imply that judges, applying general principles of the law, cannot elaborate and claim that there can be no crime if there is no damage. Take, for instance, Article 183 of the Argentinean Criminal Code, which establishes:

> ... it will be punished with prison of 15 days to a year, whomever destroys, makes unusable and disappears or in any way damages a thing ... as long as the act does not constitute a more serious offense. In the same offense will incur whomever alters, destroys or makes unusable data, documents, programs or information systems; or sells, distributes or disseminates, or introduces in an information system, a program aimed at causing damages.

[23] Article 202.1 of Ecuador Criminal Code.

[24] On this issue, see EFF, *Vulnerability Reporting FAQ*, at https://www.eff.org/issues/coders/vulnerability-reporting-faq#faq2.

[25] Article 274G of the Guatemalan Criminal Code. He shall be punished with imprisonment of six months to four years, and a fine of two hundred to one thousand quetzales, to distribute or put into circulation programs or instructions destructive, that may cause prejudice to records, programs or computer equipment.

Argentinean prosecutors questioned software developer Joaquín Sorianello under this broad and vague language after he uncovered a vulnerability in computers used by MSA, the company in charge of providing hardware and software used for official elections in the city of Buenos Aires.[26] After the government uncovered his identity through forensic analysis, the Metropolitan Police seized his computers and other work materials and placed him under criminal investigation for over a year.

In August 2016, the government dropped the prosecution against him.[27] The decision outlined the reasons for abandoning the case:

> From the analysis produced by Officer Camero of the Metropolitan Police, it comes out that from the computers seized in Sorianello's apartment more than 91 accesses to the server 'caba.operaciones.com.ar' were detected, with the creation of a [('p0wned'] event. However, no sensible data or file of interest was found which belonged to the company affected. The officer explained that [p0wned] meant, in computer culture, that a small party (a person) finds a vulnerability in a bigger party (a company), and it is usual for the small party to leave a flag, as a symbol, to let the developer know that the software is vulnerable. This flag creates no damage whatsoever, neither it alters the normal functioning of the system involved. This information is ratified by the conversation held by Sorianello and [censored section in the original], an employee from the company, [a conversation which] has been audited ... In conclusion, of the elements approached to this inquiry, it comes out that even though Joaquín Sorianello did access the systems of Grupo MSA, it did not do so to cause damage but, on the contrary, to let the company know that its security system was flawed and could be easily violated.[28]

The decision is significant for two reasons. First, the judge adequately interprets the legal regime and demands damage as a necessary element of the crime, holding that the kind of access performed by Sorianello has social utility, for it alerts those responsible for important services—in this case, for the software and hardware used in elections—of vulnerabilities that put the systems in danger.

Second, the decision was the outcome of a year-long inquiry during which the government seized and held the materials used by Sorianello in his daily work. This severe penalty suggests that it is not enough for judges to interpret the law and demand, for instance, that the government prove actual damages as a necessary element of unauthorized access. It is also necessary for the law to protect the activities of security researchers, which can be jeopardized by lengthy prosecutions that disrupt the daily lives of persons who are performing, as the judge recognizes, socially useful work that

[26] La Nación, *Detectó Fallas En El Sistema de Boleta Electrónica Y Allanaron Su Casa*, La Nación (2015).

[27] La Nación, *Sobreseyeron Al Programador Que Reveló Fallas En El Sistema de Voto Por Boleta única Electrónica*, La Nación (2016).

[28] Poder Judicial de la Ciudad de Buenos Aires, *Carta Documento de Desistimiento de Acción Penal*, Joaquín Soraniello (2016).

should be encouraged instead of punished. A legal framework that puts researchers under risk of prosecution creates the wrong incentives for good information security practices.

Canadian courts have similarly held that the law's provisions should be limited to "behaviour that a reasonable person in the circumstances of the defendant would consider a 'dishonest activity.'"[29] In spite of this limitation, however, Canada's provisions can have a chilling effect on legitimate security research. For example, in 2014, a security researcher revealed he had accessed government computer systems for the purpose of demonstrating that a widely known vulnerability could be used against Canadians filing their taxes.[30]

As a result, Canada's tax filing deadline was delayed for a week until the vulnerability was patched. The security researcher's positive intentions, however, did not prevent him from being charged with cybercrime offenses (though the researcher received a relatively light sentence).[31]

These incidents demonstrate how poorly-written or misinterpreted cybercrime law can stigmatize well-intentioned security researchers and discourage them from conducting their work for fear of criminal prosecution.

The Principle of Legality as a Guarantee of the Inter-American System

One of the main guarantees the American Convention of Human Rights grants is the legality principle. This right is supported by Article 30, which establishes:

Scope of Restrictions. The restrictions that, pursuant to this Convention, may be placed on the enjoyment or exercise of the rights or freedoms recognized herein may not be applied except in accordance with laws enacted for reasons of general interest and in accordance with the purpose for which such restrictions have been established.

[29] *R v Livingston*, 2017 ONCJ 747, (Ontario Court of Justice), para 64.

[30] Jennifer O'Brien, "*Exposing Security Flaw Forced Tax Agency to Fix it, Experts Argue",* The London Free Press, April 21, 2014, http://www.lfpress.com/2014/04/17/rcmp-not-commenting-on-harassment-accusations-from-stephen-arthuro-solis-reyes-lawyer.

[31] CBC News, "*Stephen Arthuro Solis-Reyes Charged in Heartbleed SIN Theft*", CBC News, April 16, 2014, http://www.cbc.ca/news/politics/stephen-arthuro-solis-reyes-charged-in-heartbleed-related-sin-theft-1.2612526; Jane Sims, "*Canada Revenue Agency Hacker Pleads Guilty, Says He Had Best of Intentions*", Ottawa Citizen, May 6, 2016, http://ottawacitizen.com/news/local-news/canada-revenue-agency-hacker-pleads-guilty-says-he-had-best-of-intentions.

The Court developed the meaning of the legality principle in Consultative Opinion 8/86, which interpreted the term "laws." A strict interpretation would have limited legitimate restrictions to human rights to laws passed by the legislative branches of member states. A broad interpretation would have accepted that other legal instruments, such as presidential decrees, could permit restrictions on rights.[32] In OC6/86, the Court opted for a strict interpretation of the legality principle, significantly broadening the scope of protection granted by the American Convention by ensuring that any restrictions to basic rights should only be established by a law passed by the Legislature in accordance with the Constitution.

The Court held:

> In order to guarantee human rights, it is therefore essential that state actions affecting basic rights not be left to the discretion of the government but, rather, that they be surrounded by a set of guarantees designed to ensure that the inviolable attributes of the individual not be impaired. Perhaps the most important of these guarantees is that restrictions to basic rights only be established by a law passed by the Legislature in accordance with the Constitution. Such a procedure not only clothes these acts with the assent of the people through its representatives, but also allows minority groups to express their disagreement, propose different initiatives, participate in the shaping of the political will, or influence public opinion so as to prevent the majority from acting arbitrarily. Although it is true that this procedure does not always prevent a law passed by the Legislature from being in violation of human rights—a possibility that underlines the need for some system of subsequent control—there can be no doubt that it is an important obstacle to the arbitrary exercise of power.[33]

In addition, the legality principle establishes that vague and ambiguous standards are an impermissible basis to restrict rights. The Inter-American system has a three-prong test to assess restrictions on freedom of expression. The Inter-American Commission has said, for instance, that:

> ... vague or ambiguous legal provisions that grant ... very broad discretionary powers to the authorities, are incompatible with the American Convention, because they can support potential arbitrary acts that are tantamount to prior censorship or that establish disproportionate liabilities for the expression of protected speech. Vague, ambiguous, broad or open-ended laws, by their mere existence, discourage the dissemination of information and opinions out of fear

[32] Presidential decrees, as an example, are relevant for they were the main concern of the Court when interpreting the term "laws" in OC6/86. In Latin America there is an extended practice of "legislative delegation" which grants presidents broad legislative authority, something the Court found incompatible with the Convention if through this delegation rights are restricted.

[33] La expresión "Leyes" en el artículo 30 de la Convención Americana sobre Derechos Humanos. Opinión Consultiva OC-6/86., Serie A (1986), par. 22.

> of punishment, and can lead to broad judicial interpretations that unduly restrict freedom of expression. *As such, the State must specify the conduct that may be subject to subsequent liability in order to prevent adverse impacts upon the free expression of protest and disagreement with the actions of the authorities.* When limits on freedom of expression are established by criminal laws, the Court has established that they must satisfy the principle of strict legality: ‘should the restrictions or limitations be of a criminal nature, it is also necessary to strictly meet the requirements of the criminal definition in order to adhere to the *nullum crimen nulla poena sine lege praevia* principle.’ The latter is expressed in the need ‘to use strict and unequivocal terms, clearly restricting any punishable behaviors,’ which requires ‘a clear definition of the incriminated behavior, setting its elements and defining the behaviors that are not punishable or the illicit behaviors that can be punishable with non-criminal measures.’ The Court has also pointed out that in the case of military criminal regulations, these ‘must clearly set forth without any ambiguities, inter alia, which criminal offenses fall within the specific military scope, and the illegal nature of criminal offenses by means of a description of the injury to or endangerment of military legal interests which have been seriously attacked, which may justify the exercise of punitive military power, as well as establish the appropriate sanction.’ In sum, in the judgment of the Court, a crime must be formulated ‘previously, in an express, accurate, and restrictive manner,’ because ‘criminal law is the most restrictive and severe mean to establish liabilities for illicit behavior, taking into account that the legal framework shall provide juridical certainty to citizens’[34] [emphasis added].

This legality principle conflicts with laws that base “unauthorized” access—and therefore criminal hacking—on violations of website terms of service (TOS). If that were to be accepted, legislation would delegate on unilateral private parties’ arrangements the very definition of the conduct which, according to the legality principle, must be carefully and precisely defined by the Legislature. That would violate the legality principle and the first step of the three-prong test used by the Inter-American system to assess restrictions on freedom of expression (and other rights).

Internet service providers and other online companies typically require users to agree to their TOS. TOS agreements—which almost no one reads[35]—can prohibit things like registering an account with false information, sharing a password, using automated tools to access information from the website, or accessing the site while under the age of 18.

TOS agreements can be riddled with mistakes or overbroad language, a reality which makes relying on them to assess the scope of conduct permitted or prohibited by law

[34] CIDH, *Marco Jurídico Interamericano Del Derecho a La Libertad de Expresión*, III.70-72.

[35] See David Berreby, *Click to agree with what? No one reads terms of service, studies confirm*, The Guardian, March 2017, https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print

even more problematic. Usually drafted by cautious lawyers, TOS agreements generally pretend to guard the service provider against possible liabilities, and use expansive language aimed at covering many hypothetical situations, an approach with—on occasions—can lead to absurd results. For example, Seventeen, a fashion magazine whose readers' average age is 16 and a half, had a TOS provision that said, "YOU MAY NOT ACCESS OR USE THE COVERED SITES OR ACCEPT THE AGREEMENT IF YOU ARE NOT AT LEAST 18 YEARS OLD."[36] If using a website in violation of the TOS were unauthorized access, then most Seventeen readers would suddenly become criminals. (After media attention Seventeen magazine changed its TOS language).[37]

Violations of these contractual computer use agreements should not be a crime. Governments, not private companies, must determine the scope of criminal law. But in some jurisdictions, such as the United States, outdated and vague computer crime laws have been interpreted by courts to criminalize violations of these contractual computer use policies.

These interpretations are notoriously problematic, as they threaten to turn millions of ordinary Internet users around the world into criminals on the basis of innocuous online activities, fail to give fair notice of what conduct is actually criminal, and allow prosecutors discretion to enforce the law in an arbitrary and discriminatory manner. These interpretations have also allowed companies to use computer crime laws as a tool to stifle competition.

The most notorious of the U.S. computer crime laws is the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, a 1986 criminal anti-"hacking" statute intended to target computer break-ins. The law makes it a crime to access information on a "protected computer"—which includes any computer connected to the Internet— "without authorization" or to "exceed (…) authorized access."

The CFAA does not define what it means to access a computer with or without authorization. This has created uncertainty and confusion for security researchers and ordinary Internet users. Even courts cannot agree.

While some U.S. jurisdictions have allowed CFAA liability for violations of an employer's or website's computer use restrictions, three federal courts of appeal have wisely limited the CFAA to violations of technological (code-based) "access restrictions" and not

[36] *See* Dave Maass, Trevor Timm*, Are You A Teenager Who Reads News Online? According to the Justice Department, You May Be a Criminal,* EFF, April 2013, https://www.eff.org/deeplinks/2013/04/are-you-teenager-who-reads-news-online-according-justice-department-you-may-be

[37] *See* Dave Maass, Trevor Timm, Kurt Opsahl, *Until Today, If You Were 17, It Could Have Been Illegal To Read Seventeen.com Under the CFAA,* EFF, April 2013, https://www.eff.org/deeplinks/2013/04/until-today-if-you-were-17-it-could-have-been-illegal-read-seventeencom-under-cfaa.

violations of written "use restrictions."[38] In *United States v. Nosal (Nosal I)*, the U.S. Ninth Circuit Court of Appeal rejected a broad interpretation of the CFAA, reasoning that "describing yourself as 'tall, dark and handsome,' when you're actually short and homely" on a dating site should not land you in jail.[39]

The confusion in the courts has enabled companies to abuse the CFAA's civil enforcement provision to go after any behavior they don't like—usually the behavior of a competitor—simply because a computer is involved, even in cases where there is no clear computer break in. These companies are seeking to transform the CFAA from a law meant to target malicious computer break ins into a tool for policing Internet use.
For example, *Facebook v. Power Ventures*,[40] a civil CFAA case, involved a start-up social media aggregator's consensual use of Facebook users' passwords to access their Facebook accounts on their behalf. Facebook users voluntarily shared their Facebook usernames and passwords with Power Ventures so that it could access their accounts and provides its services. Facebook objected and sent Power Ventures a cease and desist letter, citing violations of its terms of use. It also blocked one of Power Ventures' IP addresses, which was not effective because the company used multiple IP addresses. Power Ventures continued to use the passwords, as authorized by the Facebook users, and Facebook sued.

Despite there being no computer break in—no actual "hacking"—the Ninth Circuit nevertheless found Power Ventures liable for violating the CFAA by continuing to access Facebook after receiving the cease and desist letter and despite Facebook's instituting an IP address block.

The appeals panel attempted to find a middle ground in the interpretation of the CFAA, holding that the "authorization" provided to Power Ventures by an individual Facebook user could for purposes of the CFAA be rescinded by Facebook, even if the user's authorization to access their account continued. Thus, while rejecting that violations of the TOS alone could be sufficient, the court found that after receipt of the cease and

[38] Some companies have tried to get around this by phrasing computer use restrictions as access restrictions (i.e., stating "you are only authorized to access this database for work-related purposes" in place of "you may only use this database for work-related purposes"). In jurisdictions that have limited the CFAA to access retractions, courts have rejected attempts by companies to transform contractual computer use restrictions into access restrictions in this way.

[39] *See United States v. Nosal* (*Nosal I*), 676 F.3d 854 (9th Cir. 2012). This clear holding was complicated by a subsequent decision in the same case, which held (2-1) that an ex-employee had violated the CFAA when he used a current employee's password (with her permission) to access a proprietary corporate database. *United States v. Nosal (Nosal II)*, 844 F.3d 1024 (9th Cir. 2016). As Judge Reinhardt wrote in his dissent, there is no "workable line" separating "the consensual password sharing in [Nosal II] from the consensual password sharing of millions of legitimate account holders, which may also be contrary to the policies of system owners." Id. at 1049 (Reinhardt, J., dissenting). The tension between these two decisions has caused further confusion about the scope of the CFAA in the Ninth Circuit.

[40] *Facebook, Inc. v. Power Ventures*, 844 F.3d 1058 (9th Cir. 2016)

desist letter, Power Ventures was no longer accessing Facebook's computers with "authorization" under the CFAA and was committing a crime—despite having ongoing authorization from Facebook's users to access their accounts via their still-valid login credentials.

Almost immediately after the decision was handed down in 2016, other companies started sending their competitors cease and desist letters purporting to revoke "authorization" to access publicly available information on the open Internet. In 2017, in a case arising out of one of these cease and desist letters from LinkedIn, a federal district court in California recognized that "the broad interpretation of the CFAA advocated by LinkedIn, if adopted, could profoundly impact open access to the Internet."[41] This case is now on appeal, and there are multiple other cases across the country involving attempts to use the CFAA to block competitor's access to publicly available information on the Internet, stifle follow-on innovation, and limit consumer choice.[42]

More courts, however, are expressing concern over the effect a broad interpretation of the CFAA will have on open access to information on the web. In April 2018, another federal district court judge, in Washington, D.C., also recognized that a broad reading of the CFAA "threatens to burden a great deal of expressive activity, even on publicly accessible websites."[43] The case involves a group of discrimination researchers, computer scientists, and journalists who want to use automated access tools to investigate companies' online practices and conduct audit testing. However, the automated web browsing tools they want to use (often called "scraping" tools) are prohibited by the targeted websites' terms of service.

Given the uncertainty created by the CFAA's vague language and its sweeping application in some jurisdiction, the plaintiffs refrained from using automated tools out of fear of prosecution. The plaintiffs ultimately challenged the CFAA in court, arguing that the law chilled their constitutionally protected research and journalism.

[41] *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

[42] See, e.g., *RyanAir DAC v. Expedia Inc.*, 2:17-cv-01789-RSL, Dk. 1, Complaint, ¶¶ 33–70 (W.D. Wash, filed Nov. 29, 2017) (alleging a CFAA violation for accessing Ryanair's website using automated tools, in violation of Ryanair's terms of service and following receipt of cease and desist letters); *Southwest Airlines Co. v. Roundpipe LLC*, No. 3-18-cv-00033-G, Dk. 1, Complaint, ¶¶ 45–63 (N.D. Tex, filed Jan. 31, 2018), (alleging a CFAA violation for accessing fare data on Southwest's website using automated tools, in violation of Southwest's terms of service and following receipt of cease and desist letters); see also *Ticketmaster v. Prestige Entertainment*, No. 217-cv-07232, 2018 WL 654410, at *6 (C.D. Cal. Jan. 31, 2018) ("Ticketmaster contends that Defendants lacked or exceeded their authorization by violating its TOS, even after it sent Defendants a cease-and-desist letter outlining the alleged violations[,]" via its continued using automated software to circumvent CAPTCHAs).

[43] *Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *15 (D.D.C. Mar. 30, 2018).

The court found that the CFAA must be interpreted narrowly to avoid running afoul of the First Amendment. It ruled that the CFAA does not criminalize accessing information in a manner that the website owner does not like if you are otherwise entitled to access that very same information. And according to the court, "[s]craping or otherwise recording data from a site that is accessible to the public is merely a particular use of information that plaintiffs are entitled to see."[44] As the court explained:

> Scraping is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions.[45]

Similarly, Canadian authorities announced on May 7, 2018 that they dropped all charges against a 19-year-old Canadian they had previously accused of unauthorized use of a computer service for downloading public records from a government website. These documents were hosted on the government web server that also hosted public records containing no personal information. Every request hosted on the server contained very similar URLs, which differed only in a single document ID number at the end of the URL. The teenager took a known ID number, and then, by modifying the URL, retrieved and stored all of the FOIA documents available on the Nova Scotia FOIA website.[46]

Latin American TOS often include language that outlines the course of action a company might take if their TOS is violated. Consider the case, for instance, of Mercado Libre, a popular site for buying and selling goods in Latin America. In its Argentinian version, Mercado Libre's TOS provides numerous restrictions on its users:

> Prohibitions. The users will not be able to: (a) manipulate the prices of the articles; (b) to maintain any type of communication by e-mail, or by any other means (including social networks) during the offer of the good with any of the Users that participate in it, except in the Questions and Answers section; (c) disclose your personal or other users' information through the Q & A section and / or by some other means (including but not limited to Twitter, Facebook and / or any other social network), except as specifically provided For the category Cars, motorcycles and others, Services and Properties and Properties; (d) accept personal data provided by other users through the Questions and Answers section and / or some other means (including but not limited to Twitter, Facebook and / or any other social network); (e) publish or sell prohibited articles under the General Terms and Conditions, other Free Market policies or current laws; (F) insulting or assaulting other Users; (g) use your reputation, ratings or

[44] *Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *16 (D.D.C. Mar. 30, 2018).

[45] *Sandvig v. Sessions*, No. CV 16-1368 (JDB), 2018 WL 1568881, at *7 (D.D.C. Mar. 30, 2018).

[46] Katitza Rodriguez, Aaron MacKey, *Dear Canada: Accessing Publicly Available Information on the Internet Is Not a Crime*, EFF, April 19, 2018. https://www.eff.org/deeplinks/2018/04/dear-canada-accessing-publicly-available-information-internet-not-crime

> comments received on the Free Market site in any area outside of Free Market; (h) publish identical articles in more than one publication; (i) publish identical products in more than one publication. This type of activity will be investigated by Mercado Libre and the infringer may be sanctioned with the suspension or cancellation of the offer and even of its registration as a Free Mercado Libre user and / or in any other way that it deems pertinent, *without prejudice to the actions Legal grounds that may result in the configuration of crimes or misdemeanors or civil damages that may cause to users offering.*[47]

As far as we know, there are no criminal cases initiated in Latin America where it has been argued that the violation of TOS fulfills the requirement of a computer crime. Nevertheless, TOS are worded such that companies place responsibility on users for the use of their services.

To illustrate this, we compare three services in three countries: Argentina, Colombia, and Mexico. In the case of Argentina, we will analyze Mercado Libre and OLX. Both are popular services for buying and selling merchandise. In all cases, TOS are written in a way that closely follows the legal usage for contracts in Latin America. For instance, the contractual nature of Mercado Libre’s Argentinian Terms and Conditions suggest that the responsibilities involved in their violation include civil, not criminal, liability:

> This agreement describes the general terms and conditions (the ‘General Terms and Conditions’) applicable to the use of the services offered by Mercado Libre SRL, CUIT 30-70308853-4, (‘the Services’) within the sites www.mercadolibre (‘User’ or in the plural ‘Users’) who wishes to access and / or use the site or the Services. You may do so subject to the respective General Terms and Conditions, together with all other policies and principles governing Free Market and are incorporated herein by reference.[48]

[47] See *Mercado Libre*, TOS, available (in Spanish) at: http://ayuda.mercadolibre.com.ar/ayuda/terminos-y-condiciones-de-uso_991.

[48] See *Mercado Libre*, TOS, available (in Spanish) at: http://ayuda.mercadolibre.com.ar/ayuda/terminos-y-condiciones-de-uso_991.

The same happens with OLX in Argentina,[49] with Mercado Libre in Colombia[50] and with Linio (a retail store) in México.[51] For civil enforcement under general contract law, courts could award the website damages for TOS violations.

However, under the legality principle, TOS provisions cannot be used to meet the vague and ambiguous standards established in criminal provisions (for example, "without authorization"). Criminal liability cannot be based on how private companies would like their services to be used. On the contrary, criminal liability must be based on laws which describe in a precise manner which conduct is forbidden and which is punishable. Furthermore, even civil liability could be considered a violation of freedom of expression if is disproportionate.[52]

Following general principles of criminal law, all criminal provisions should be interpreted narrowly: an interpretation which links an ambiguous term to broad contractual arrangements defined unilaterally by one of the parties of this contract would be overly broad—and therefore incompatible with the American Convention of Human Rights.

General Principles of Criminal Law

In Latin America, general principles of criminal law share two main sources: legal scholarship, and international human rights standards.

As in any continental system of law, what legal scholars have to say regarding a legal regime is usually of paramount importance. Their works are widely distributed and judges use legal scholar's ideas for arguing cases. Furthermore, judicial decisions are generally not very important for learning the law. Instead, scholars expound and systematize and that is how knowledge within the legal field is reproduced.[53]

[49] "OLX S.A. Offers a series of online resources that include classified ads, forums and different communication services ('the Services'), all subject to these Terms of Use ('Terms' or 'Terms')". See *OLX*, TOS, available (in Spanish) at: https://help.olx.com.ar/hc/es-419/articles/209280286-Condiciones-de-Uso.

[50] "This agreement describes the terms and conditions (the 'Terms and Conditions') applicable to the use of the services offered by MercadoLibre Colombia S.A. Within the site www.mercadolibre.com.co 'MercadoLibre' or the 'site') for your product 'MercadoShops' ('the Service')". See *Mercado Libre* (Colombia), TOS, available at: http://www.mercadolibre.com.co/jm/ml.faqs.portalFaqs.FaqsController?axn=verFaq&categId=SGART&faqId=5640.

[51] "These terms and conditions regulate the use of the website www.linio.com.mx, of which Bazaya México, S. de R.L. Of C.V., is owner, which is a Limited Liability Company with Variable Capital, with address at Rio Elba No. 20, Piso 5, Colonia Cuauhtémoc, Cuauhtémoc Delegation, C.P. 06500, in Mexico City". See *Linio*, TOS, available (in Spanish) at: https://www.linio.com.mx/sp/terminos-y-condiciones.

[52] *Id.*, par. 110.

[53] Pierre Bourdieu, *Force of Law: Toward a Sociology of the Juridical Field, The*, 38 Hastings LJ 805, 821 (1987).

This traditional focus on legal scholarship has receded in the last few decades, partially in favor of an understanding of law which is most linked to the role of the Constitution within the legal system, an approach which in Latin America—as in some countries of Europe—has been called *neo-constitutionalism*.[54]

The neo-constitutionalism approach considers that the constitution of a given country is the paramount law of the land. Neo-constitutionalism is response to the increasing internationalization of the law, which in Latin America happened mostly through the Inter-American system of human rights. The idea that international human rights law is *superior* to national law has been so recognized by several courts in Latin America and several constitutions establish this principle.

Therefore, international human rights standards have become a very important source of general principles of criminal law—and that is the second, more recent source we should focus on, for two reasons. First, doctrine used to be extremely national. While legal transplants and borrowing happened in Latin America, some systems were more influenced by some schools of thought, some more by others, and so on.

Second, international human rights law develops, within the Inter-American system, through the case-law that the IA Court and the IACHR have developed over the course of decades. This means that what the system has to say about criminal law principles usually comes from interpretations of relevant human rights recognized in the American Convention, and these interpretations are deployed in dialogue with national decisions which may or may not have considered the international standards.

Sources of Criminal Law Principles

So what are the general principles of criminal law developed by the Inter-American system of human rights? Where do they come from and how do they apply to the many ways in which criminal law can be used to override the rights of coders?

The American Convention is the main source of criminal law principles that deal with criminal matters, especially Article 8, which guarantees the *right to a fair trial*:

> Article 8. Right to a Fair Trial. 1. Every person has the right to a hearing, with due guarantees and within a reasonable time, by a competent, independent, and impartial tribunal, previously established by law, in the substantiation of any accusation of a criminal nature made against him or for the determination of his rights and obligations of a civil, labor, fiscal, or any other nature. 2. Every person accused of a criminal offense has the right to be presumed innocent so long as his guilt has not been proven according to law. During the proceedings, every person

[54] Miguel Carbonell, Teoria del neoconstitucionalismo. Ensayos escogidos (TROTTA, 2007); Miguel Carbonell & Leonardo García, El canon neoconstitucional (2010); Eduardo Aldunate Lizana, *Aproximación Conceptual Y Crítica Al Neoconstitucionalismo*, 23 Revista de derecho (Valdivia) 79 (2010).

> is entitled, with full equality, to the following minimum guarantees: a. the right of the accused to be assisted without charge by a translator or interpreter, if he does not understand or does not speak the language of the tribunal or court; b. prior notification in detail to the accused of the charges against him; c. adequate time and means for the preparation of his defense; d. the right of the accused to defend himself personally or to be assisted by legal counsel of his own choosing, and to communicate freely and privately with his counsel; e. the inalienable right to be assisted by counsel provided by the state, paid or not as the domestic law provides, if the accused does not defend himself personally or engage his own counsel within the time period established by law; f. the right of the defense to examine witnesses present in the court and to obtain the appearance, as witnesses, of experts or other persons who may throw light on the facts; g. the right not to be compelled to be a witness against himself or to plead guilty; and h. the right to appeal the judgment to a higher court. 3. A confession of guilt by the accused shall be valid only if it is made without coercion of any kind. 4. An accused person acquitted by a non appealable judgment shall not be subjected to a new trial for the same cause. 5. Criminal proceedings shall be public, except insofar as may be necessary to protect the interests of justice.

In addition, certain guarantees come out from the American Convention itself:

> **Independent courts**. Article 8.1 guarantees the right to be judged by a competent tribunal, previously established by law. This relates to the concept of natural judge, [55] one of the due process guarantees.[56] It should be noted that this guarantee also applies to legislative and administrative authorities insofar as they are entitled to make decisions that affect the rights and obligations of citizens.[57]
>
> **Presumption of innocence**. Article 8.2 demands that '[e]very person accused of a criminal offense has the right to be presumed innocent so long as his guilt has not been proven according to law.'[58] Furthermore, the *onus probandi* lies within the state, in charge of the accusation.[59] The Inter-American Court has also stated that the presumption of innocence means that persons accused must be treated as such, which means that, for example, jail time before a definitive decision violates not only the right to personal freedom but also the presumption of innocence, especially when it exceeds a reasonable time.[60]

[55] In continental law systems, the *natural* judge is the judge who is in supposed to intervene in a given controversy according to the preexisting rules governing jurisdiction.

[56] Case of *Barreto Leiva v. Venezuela*, Serie C (2009), par. 75.

[57] Case of *Tribunal Constitucional (Camba Campos y otros) vs. Ecuador*, Serie C (2013), par. 71.

[58] *Ricardo Canese v. Paraguay*, Serie C (2009), par. 153.

[59] *Id.*, par. 154.

[60] *Caso Loayza Tamayo v. Perú*, Serie C (1997).

Equality of resources.[61] The Inter-American Court has claimed that the inequality which usually exists in criminal procedures must be dealt with in positive measures. In that sense, the Inter-American Court has stated that those subject to a criminal procedure must be in a position to exercise their rights and defend their interests in an effective manner, in conditions of equality with other persons involved in the procedure. Conditions of inequality demand that measures for compensation be adopted. These measures involve, for instance, the presence of translators for those who don't know the language in which the procedure is taking place.[62]

Legality principle. As more fully discussed above, this is a basic principle according to which everything that is not expressly forbidden, is permitted. It is called the legality principle or—sometimes—the principle of reserve. The principle is established by Article 9 of the American Convention, which states that "[n]o one shall be convicted of any act or omission that did not constitute a criminal offense, under the applicable law, at the time it was committed. A heavier penalty shall not be imposed than the one that was applicable at the time the criminal offense was committed." In this sense, the Inter-American Court has stated that criminal judges must apply the law strictly, and must pay special attention to match the conduct with the legal description of the offense.[63] In the Consultative Opinion 8/86, the Court stated that the legality principle is closely linked to the need that offenses and restrictions to human rights are clearly established by law, which means an official act by the body in charge of the legislative power.

Proportionality in punishment. The Inter-American Court has also stated that punishments must be proportional. In that sense, the Court has established that punishment must be proportional to the juridical good that was affected and the degree of guilt with which the offender acted. Therefore, punishment must be in relation to the nature and seriousness of the offense.[64]

Criminal Law Principles and Cybercrime Legislation in Latin America

From the general principles of criminal law in Latin America, three are especially relevant to a discussion of coders' rights: the principle of legality, equality of resources, and proportionality in punishment. The principle of legality was covered in previous sections, when *coding* was analyzed under the light of Article 13 of the American

[61] This term comes from Spanish, and is related to the idea that in a duel, both contenders should have access to the same kind of weapon. The *equality of arms* principle has been translated as equality of resources, but it is closely linked to the principle *audi alteram partem*, a basic requirement of due process.

[62] *Caso Acosta Calderón v. Ecuador*, Serie C (2005), par. 195.

[63] *Caso García Asto y Ramírez Rojas v. Perú*, Serie C (25 NOV 2005), par. 190-195.

[64] *Caso Ximenes Lopes v. Brasil*, Serie C (2006), par. 108.

Convention. The principles of *equality of resources and proportionality* in the American Convention also can protect the rights of coders.

Equality of Resources

The *equality of resources* principle is the procedural guarantee of fairness of an adversarial procedural system as known in continental law systems. The principle has special salience in the case of cybercrime offenses, for these are crimes where evidence is difficult for judges and prosecutors to understand. Even when special units exist, cybercrime offenders have the right to be treated fairly and equally, and that includes having access to specialists who can communicate in a fair and objective manner the matters of the case to judges and prosecutors. Evidence must be carefully analyzed and some sort of translation needs to take place for evidence to be understood by those who are part of the criminal process. This requirement becomes even stronger when juries are involved. The kind of *fair trial* guaranteed by Article 8 of the American Convention demands that those suspected of having committed a cyber-offense are portrayed fairly during the prosecution by having adequate access to experts who can interpret complex evidence for those who are unable to read code and understand the complexities of computer programming.

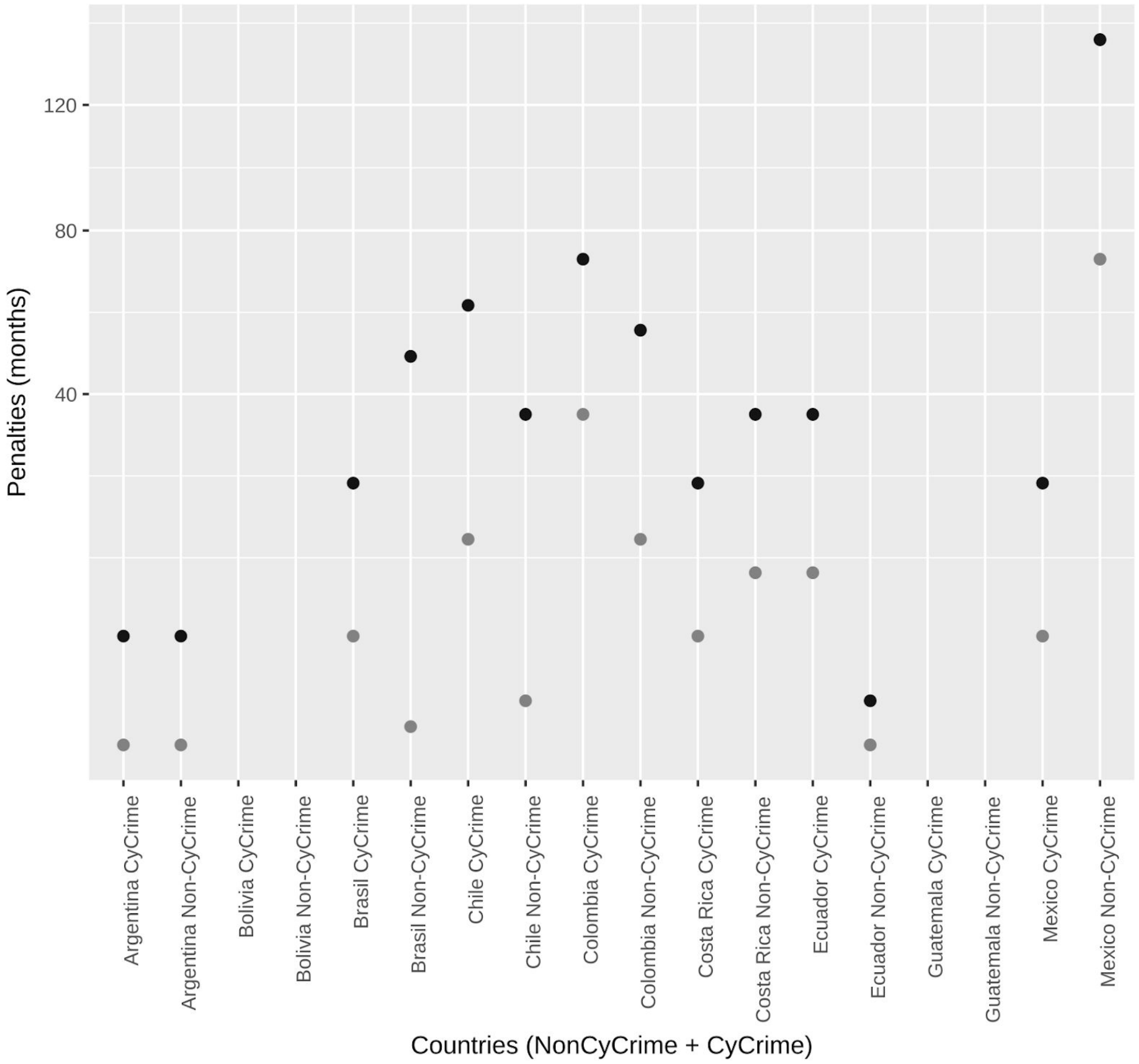
Proportionality in Punishment

According to our comparative analysis of the way Budapest Convention offenses are coded in nine countries of Latin America,[65] not all seven of the offenses were considered nor are all of them part of the legal frameworks of the countries compared.[66] However, the comparison produced interesting insights, even when weighing in generalizations and simplifications made for the analysis to be possible. For instance, when a cyber-offense was comparable to a crime which was distinguished in several sorts of actions and punished accordingly, we considered these different crimes as one in order to measure the minimums and maximums of punishments established by law. We also translated all punishments into months to simplify comparisons. The output is two numbers, one related to cyber-offenses and the other related to similar, non-cyber crimes. The outcome of this computation can be seen in Chart 1. The grey dots show the minimum penalty for illegal interception of communications in Latin America and the black dots show the maximum penalty for the same crime.

[65] These countries are Argentina, Bolivia, Brazil, Chile, Colombia, Costa Rica, Ecuador, Guatemala and México.

[66] These include illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery and computer-related fraud. We excluded child pornography. While illegal access, system interference, and misuse of devices were considered, they were excluded from the comparative exercise because no clear case of a similar, comparable non-cyber offense could be made. However, that was possible with illegal interception (1), data interference (2), computer-related forgery (3) and computer-related fraud (4). In all four cases we were able to find comparable non-cyber offenses: interception of private communications (1), damages on goods or property (2), falsification of documents (3) and fraud (4).

Chart 1. Illegal Interception in Latin America.
Computer crime (CC) and non-computer crime (NC) offenses.



In some countries, cybercrimes are punished less harshly than their non-cyber counterparts. For instance, in Brazil, the crime of "invasion of a computer device" (Article 154A of Act 12.737) is punished in a range of six months to two years. Similar, non-cyber offenses are punished with a different scale. For instance, violation of mail is punished with a maximum of six months by Article 151, but the illegal interception of telegraphic, radio-electric, or telephone conversations is punished with a maximum of three years (if an official agent is involved in the crime).[67] This is also the case in Bolivia and Ecuador.

Other countries have a more balanced approach. Argentina, for instance, punishes cyber and non-cyber offenses in the same way, with cyber and non-cyber offenses in the same section of the Criminal Code. In that sense, Article 153 and Article 153 *bis* punishes illegal access to private communications, whether communications are electronic (telephone, computers, and so on) or not (traditional mail).[68] On the other hand, Article 183 covers damages for both material and electronic goods, and establishes the same penalty for both offenses.[69] We also find a balanced approach when we look at specific crimes. For

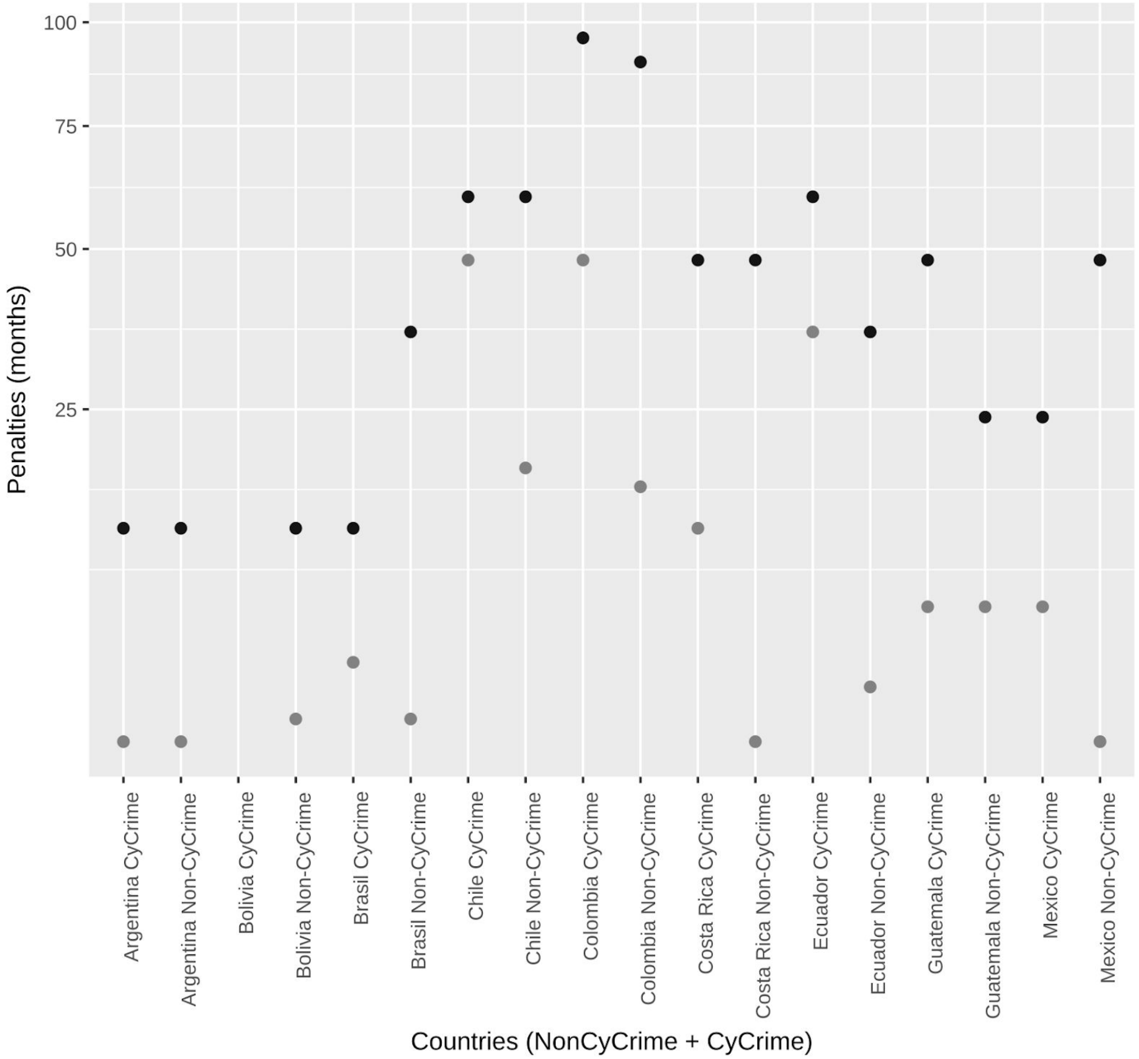
[67] *See* Article 151 of the Brazilian Criminal Code. "Breach of correspondence. Art. 151. Unduly discard the content of closed correspondence addressed to another: Penalty - detention, from one to six months, or fine. Withholding or destruction of correspondence Paragraph 1 - The same penalty shall apply: I - who improperly seizes other people's correspondence, although not closed and, in whole or in part, takes or destroys; Violation of telegraphic, radio or telephone communication II - who improperly disseminates, transmits to another person or abusively uses telegraphic communication or radio-electrical directed to third party, or telephone conversation between other people; III - who prevents the communication or the conversation referred to in the previous number; IV - who installs or uses radioelectric station or apparatus, without observing legal provision. Paragraph 2. The penalties increase by half if there is harm to another. Paragraph 3 - If the agent commits the crime, with abuse of function in postal, telegraphic, radioelectric or telephone service: Penalty - detention, one to three years. Paragraph 4 - It is only by means of representation, except in cases of § 1, IV, and 3."

[68] Argentina Criminal Code. Article 153. The person who opens or improperly agrees to an electronic communication, a letter, a closed document, a telegraphic, telephone or other office, which is not punishable by imprisonment from fifteen (15) days to six (6) months. It is directed; or improperly seized of an electronic communication, letter, sheet, office or other private role, even if it is not closed; Or unduly suppresses or diverts from its destination a correspondence or an electronic communication that is not addressed to it. The same penalty shall be incurred by any person who improperly intercepts or captures electronic communications or telecommunications from any private or restricted access system. The penalty shall be imprisonment from one (1) month to one (1) year, if the author also communicates to another or publishes the contents of the letter, writing, office or electronic communication. If the act is committed by a public official who abuses his duties, he will also suffer special disqualification for twice the time of the sentence. Article 153 BIS. - It will be repressed with imprisonment from fifteen (15) days to six (6) months, if it does not result in a crime more severely punished, which knowingly accedes by any means, without the proper authorization or exceeding what it possesses, to a system or Restricted access computer data. The penalty shall be from one (1) month to one (1) year of imprisonment where access is to the detriment of a computer system or data of a state public agency or a provider of public services or financial services.

[69] Argentina Criminal Code. Article 183. It shall be repressed with imprisonment from fifteen days to one year, which destroys, renders useless, makes disappear or otherwise injures a movable or immovable property or an animal, totally or partially alien,

instance, when considering damages produced through *data interference* crimes and damages produced when other kind of property is affected, scales seem to be quite similar, with occasional outliers. Costa Rica, Ecuador, Colombia, Chile and Guatemala, for instance, punish cyber-offenses in a slightly harsher way (see Chart 2). The grey dots show the minimum penalty for data interference in Latin America and the black dots show the maximum penalty for the same crime.

Chart 2. Data interference in Latin America.
Computer crime (CC) and non-computer crime (NC) offenses.



Several countries, however, punish cyber-offenses with harsher penalties than similar, non-cyber offenses. This is the case of Colombia, where the interception of computer

provided that the act does not constitute another crime More severely punished. The same penalty shall be incurred by anyone who changes, destroys or renders unusable data, documents, programs or computer systems; Or sell, distribute, circulate or introduce into a computer system any program designed to cause damage.

data is punished with a scale of 36-72 months,[70] while the illicit violation of private communications is punished with a scale of 16-54.[71] For crime that involves damages, cyber-offenses and non-cyber offenses are also punished differently. Article 265 punishes damages to goods which belong to someone else[72] with a scale of 16-90 months, and Article 269D punishes computer damage[73] with a scale of 48-96 months.

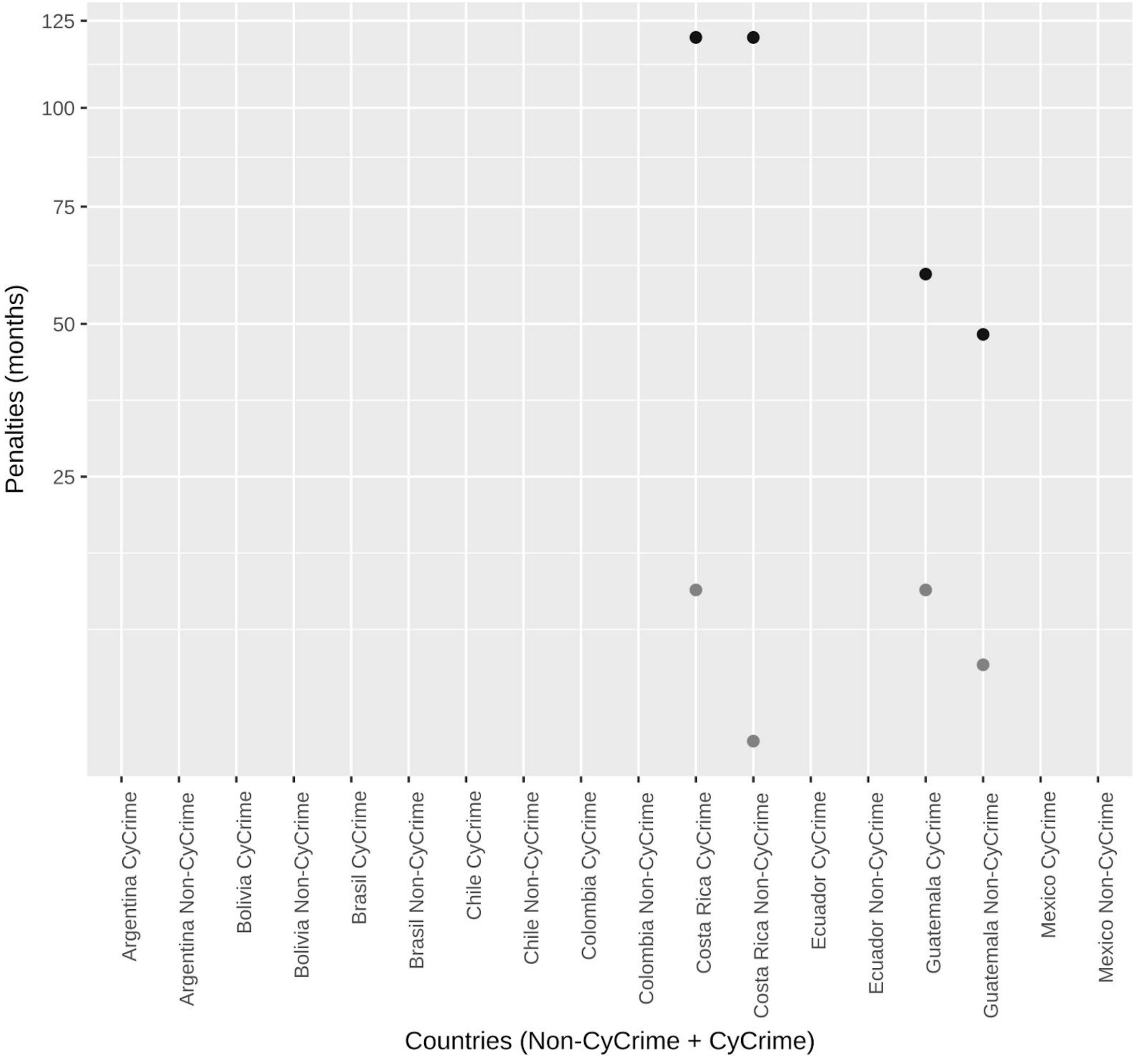
[70] Colombia Criminal Code. Article 269C. Interception of computer data. Any person who, without a previous judicial order, intercepts computer data at the origin, destination or inside a computer system, or electromagnetic emissions from a computer system that will transport them, shall be liable to imprisonment from thirty-six (36) to seventy And two (72) months.

[71] Colombia Criminal Code. Article 192. "Unlawful violation of communications. Any person who illegally abandons, conceals, misleads, destroys, intercepts, controls or prevents a private communication addressed to another person, or improperly finds its contents, shall be imprisoned from sixteen (16) to fifty-four (54) months, provided That the conduct does not constitute an offense punishable by a higher penalty. If the perpetrator reveals the content of the communication, or uses it for his own or another's benefit or to the detriment of another, the penalty shall be imprisonment from thirty-two (32) to seventy-two (72) months". It should be noted that the increase in punishment is conditioned upon the revelation of the content to a third party, its use for self-benefit or damages. Such aggravating circumstances are not necessary for the cyber-offense (Article 269C).

[72] Colombia Criminal Code. Article 265. Damage to the good of others. Any person who destroys, renders harmless, makes disappear or otherwise damages any other person, property or real property, shall be imprisoned from sixteen (16) to ninety (90) months and fined six point sixty six (6.66) to thirty seven point five (37.5) minimum legal monthly salaries in force, provided that the conduct does not constitute an offense sanctioned with a higher penalty. The penalty will be from sixteen (16) to thirty-six (36) months of imprisonment and a fine up to fifteen (15) legal minimum monthly salaries in force, when the amount of the damage does not exceed ten (10) legal minimum monthly salaries in force. If the damage caused to the offended or injured person is compensated before a first or only instance sentence is pronounced, there will be place to the resolution of inhibitory resolution, preclusion of the investigation or cessation of procedure.

[73] Article 269D. Colombia Criminal Code. Computer damage. Any person who, without being entitled to destroy, damage, erase, deteriorate, alter or delete computer data, or an information processing system or its logical parts or components, shall be liable to imprisonment of forty-eight (48) to Ninety-six (96) months and in a fine of 100 to 1,000 legal minimum monthly salaries in force.

Chart 3. Computer-related forgery in Latin America.
Computer crime (CC) and non-computer crime (NC) offenses.



The difference in the minimum penalties in particular seem unwarranted since the damage to computer data might be as mild as that done to a private person's goods or real estate.

Consider, for instance, the hacking of a web page in which no data is destroyed but a banner not authorized by the owner is put up as a form of protest.[74] This action is analogous to the spray painting of a wall of a corporate building. Assuming for the sake

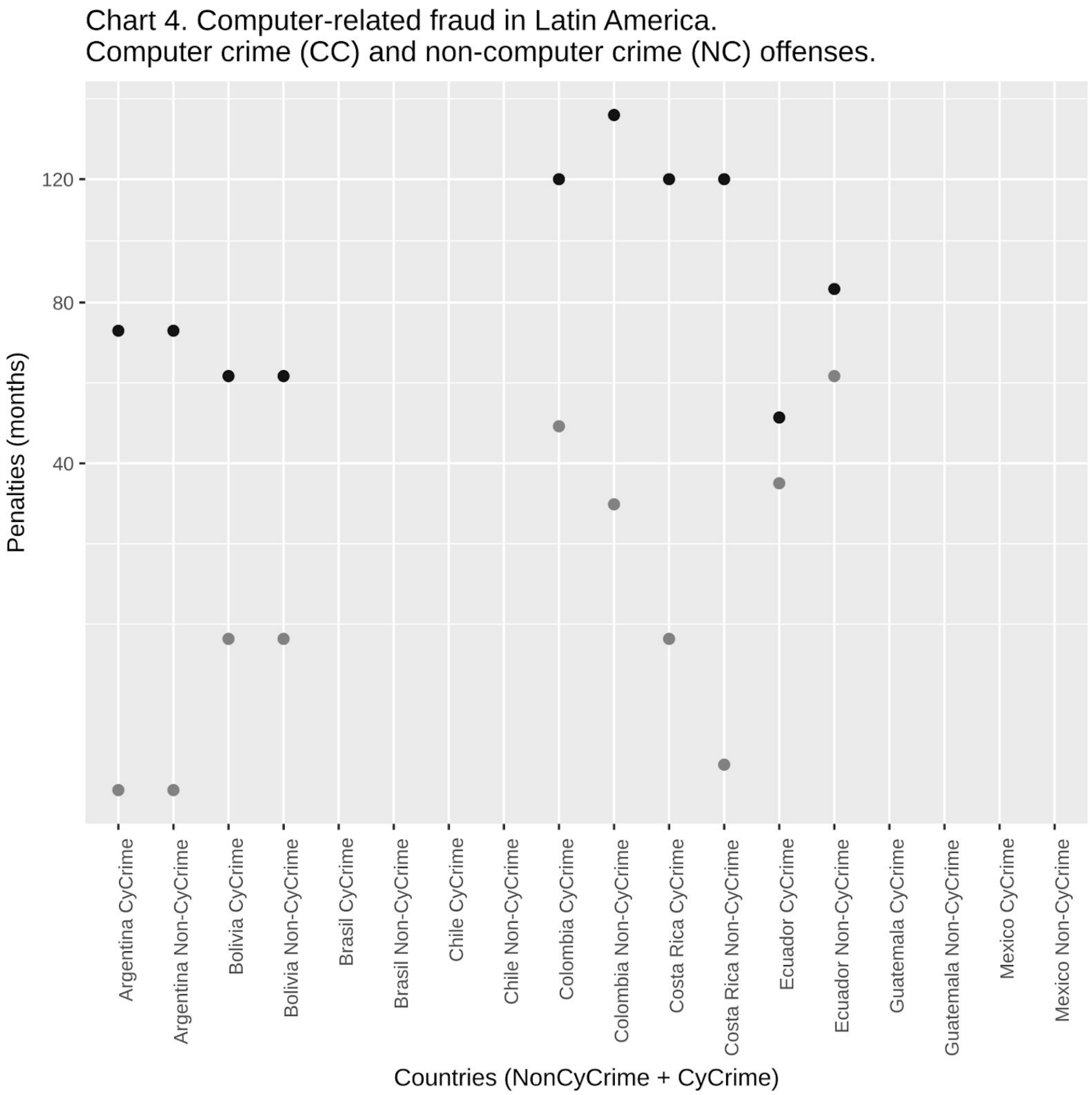
[74] See e.g. Victoria Kim, *Thomson Reuters editor Matthew Keys faces hacking charges,* L.A. Times, March 14, 2013 http://latimesblogs.latimes.com/lanow/2013/03/thomson-reuters-editor-matthew-keys-faces-hacking-charges-.html (A "hacker accessed a news story on The Times' website and changed a headline to read: 'Pressure builds in House to elect CHIPPY 1337.'") *See also* EFF, The Punishment Should Fit the Crime: Matthew Keys and the CFAA, Dec. 15, 2015, https://www.eff.org/deeplinks/2015/12/punishment-should-fit-crime-matthew-keys-and-cfaa.

of argument that the minimum penalty applies to both actions, then the outcome is unreasonable: the hacking would receive a minimum of four years in prison, while the spray paint would be punished with sixteen months.

The same kind of reasoning applies to the crime of *fraud*. When fraud is committed through a computer, it receives a penalty between 48 and 120 months in prison.[75] When the crime is committed in a different way, it receives a penalty of between 32 and 144 months.[76]

[75] Colombia Criminal Code. Article 269J. Non-consensual transfer of assets Any person who, for the sake of profit and using any kind of manipulation or similar device, obtains the non-consensual transfer of any asset to the detriment of a third party, provided that the conduct does not constitute an offense punishable by a more serious penalty, In prison sentence of forty-eight (48) to one hundred twenty (120) months and in a fine of 200 to 1,500 legal monthly minimum wages in force. The same penalty shall be imposed on whoever manufactures, introduces, possesses or facilitates a computer program intended for the commission of the offense described in the preceding paragraph, or a scam. If the conduct described in the two previous paragraphs has an amount higher than 200 legal monthly minimum wages, the penalty indicated therein will increase by half.

[76] Colombia Criminal Code. Article 246. Fraud. Any person who obtains an unlawful gain for himself or for a third party, with the prejudice of another person, inducing or keeping another in error by means of artifices or deception, shall be imprisoned from thirty-two (32) to one hundred and forty-four (144) months and a fine of sixty-six point sixty-six (66.66) to one thousand five hundred (1,500) legal minimum monthly salaries in force. In the same penalty shall be incurred in the lottery, raffle or game, to obtain profit for himself or for others, using any fraudulent means to ensure a certain result.



Another country where we found unreasonable differences is Guatemala, where data interference (see Chart 2) doubles the maximum penalty when the interference has been produced using computers. The same happens with computer-related forgery (see Chart 3)[77]. In Costa Rica, computer-related fraud is punished with a harsher penalty scale than fraud committed through other means (see Chart 4)[78].

The way conduct is punished violates the Inter-American standards, which require proportional punishments. In the cases analyzed, the juridical goods protected are comparable between cyber and non-cyber offenses. However, in some cases cyber-offenses can be more harshly punished than non-cyber ones. These

[77] The grey dots show the minimum penalty for computer-related forgery in Latin America and the black dots show the maximum penalty for the same crime.
[78] The grey dots show the minimum penalty for computer-related fraud in Latin America and the black dots show the maximum penalty for the same crime.

disproportionate penalties can harm computer security, as they discourage security research that might come under the statutes—especially when the statutes are vague.

Recommendations

A legal framework that encourages security research is essential for the well-being of the Internet and of our communications networks. As we increasingly move our public debate from traditional media to online outlets, the security of this environment becomes essential for the protection of our most fundamental human rights: freedom of expression, freedom of association, and privacy.

In Latin America, this relationship calls for applying the high standards of the Inter-American Human Rights system to the kind of activities which are, in and of themselves, a form of speech, and which are capable of guaranteeing that the Internet remains a free, open, and secure space for public debate to take place.

For that reason, EFF's Coders' Rights project will ask the Inter-American Commission of Human Rights to develop its freedom of expression and privacy standards in a way that protects coders' rights, as (a) a kind of expression which in and of itself falls within the scope of Article 13 of the American Convention and (b) as a kind of speech which deserves special protection, for it is closely linked to the openness and security of the Internet, the medium that Latin American citizens increasingly choose to engage in the kind of public debate that, as the Commission states, is the "cornerstone of any democratic society."[79]

For that reason, this project seeks to have the Inter-American Commission to develop standards that:

> Guarantee that the creation, possession, or distribution of tools designed to test or compromise the security of a system, service, or program are activities covered by Article 13 of the American Convention which should not be criminalized or otherwise restricted. These tools are critical to the practice of defensive security and have legitimate, socially desirable uses, such as identifying a practical vulnerability.
>
> Discourage the use of criminal law as a response to behavior by security researchers which, while technically in violation of a computer crime statute, is socially beneficial. In that sense, the Inter-American Commission should encourage the use of its three-prong test to analyze cases involving the activities of security researchers in a way that factors in the contribution security researchers make to keeping the Internet a free and open space. This should include the use of common security tools in research and testing.

[79] CIDH, Libertad de Expresión E Internet (Comisión Interamericana de Derechos Humanos, 2013), par. 1.

Demand that, in Member State's criminal law, the intent required for criminal liability should be beyond that of a mere intentional act, but rather include some element of maliciousness and actual damages.

Demand that penalties for crimes committed with computers should, at a minimum, be no higher than penalties for analogous crimes committed without computers. Additionally, penalties for computer crimes should be proportional to the actual harm caused.