Submission to the European Parliament on the Draft Directive on Attacks against Computer Systems

February 8, 2011

Katitza Rodriguez
International Rights Director

Marcia Hofmann
Senior Staff Attorney

EFF is an international civil society non-governmental organization with more than 16,000 members worldwide, dedicated to the protection of citizens' online civil rights, privacy, and freedom of expression. EFF engages in strategic litigation in the United States and works in a range of international and national policy venues to promote balanced laws that protect human rights, foster innovation and empower consumers. EFF is located in San Francisco, California and has members in 67 countries throughout the world.

EFF Comments on the Draft Directive on Attacks against Computer Systems

General Overview

The Electronic Frontier Foundation (EFF) is pleased to have the opportunity to submit comments on the draft Directive on attacks against information systems.

EFF is skeptical of the overall need for this draft directive. We believe the Commission has not made a strong case for its need, especially given the existence of the Council of Europe Cybercrime Convention, which has not been implemented by all of the signatory states. Indeed, only 15 out of 27 Member States have ratified the Treaty (which EFF did not agree with at the time of its passage and we continue to believe it is overly restrictive). As matter of fact, the Cybercrime Convention deal with illegal access (Article 2), illegal interception (Article 3), data interference (Article 4), system interference (Article 5), misused of devices (Article 6), computer-related fraud (Article 8), among other things, which are largely duplicated by the proposed Directive. Moreover, the current language of the draft Directive is more problematic for legal certainty and much more vague than the Convention making it even more dangerous for citizens' civil liberties.

Aside from the fact that there is already legislative protection against computer crime in Europe, the lack of implementation of the Convention does not bode well for an effective enforcement of the proposed directive. Regardless, EFF is concerned about various policy issues regarding the EU's additional attempt to criminalize what it determines to be attacks on information systems.

Vague and Overbroad Definition of 'Without Right'

First, this draft directive will affect users' free expression by restricting what they are allowed to do with computers. 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, the provisions of the draft directive may be too vague and broad regarding what constitutes criminal acts, so the draft directive as it stands may indeed constitute a disproportionate encroachment into users' free expression and the freedom to innovate and compete in the economic market. Some draft recommendations from the Rapporteur Monika Hohlmeier, which would clarify various terms, may alleviate this problem, but as the Greens/EFA's response says, some of these 'clarifications' may in fact confuse matters further.

In particular, **Article 2** remains troubling even with the amendment proposed by the Greens/EFA. 'Without right' is still defined as 'access, use [added by the Greens/EFA] or interference ***not authorized*** by the owner [or] other right holder of the system' (emphasis added).

This definition resembles language in the US Computer Fraud and Abuse Act (CFAA), which provides, among other things, that it is illegal to 'intentionally access[] a computer ***without***

authorization or ***exceed[] authorized access***, and thereby obtain[] . . . information from any protected computer.' (emphasis added).[1]

The precise scope of the phrases 'without authorization' and 'exceeds authorized access' has been hotly disputed in the courts, with the US government and private companies arguing for a broad interpretation that would go so far as to criminalize violations of private contractual agreements. (The CFAA is both a civil and criminal statute, which means that both private parties and federal prosecutors can pursue violations.) If followed by courts in Europe, this approach threatens to put the immense coercive power of criminal law in the hands of those who draft contracts. This means that private parties, rather than lawmakers, would be in a position to determine what conduct is criminal—simply by prohibiting it in an agreement. That is particularly troubling for website terms of use, which are typically arbitrary and confusing agreements of adhesion that users may "agree" to without ever having read. Criminalizing breaches of website terms of use could turn millions of Internet users into criminals for typical, everyday activity—simply because the drafter decides that it will be so.

One of the first cases of this sort was *United States v. Drew*, in which government prosecutors claimed that a woman who signed up for a MySpace account using a fictitious name and age obtained "unauthorized access" to the service and therefore violated the CFAA because she violated MySpace's terms of service. A court ultimately determined that such an interpretation of the CFAA would render the law unconstitutionally vague, since the public would not have adequate notice about what behavior is illegal, and the government would be able to cherry-pick cases to prosecute at its whim.[2]

Unfortunately, these profound constitutional concerns have not prevented the government from continuing to argue that the CFAA criminalizes violations of terms of use. In *United States v. Lowson*, prosecutors indicted the operators of a ticket-reselling service who purchased tickets through the Ticketmaster website using automated means. The prosecutors argued that the resellers' actions violated the Ticketmaster website's terms of use, and therefore the CFAA. The defendants in the case ultimately pleaded guilty to the charges.[3]

In a similar line of cases, the government has argued that violations of corporate policies are computer crimes. For example, in *United States v. Nosal*, the government is pursuing CFAA charges against the former employee of an executive recruiting firm who convinced current employees to access the company's proprietary database and pass along information that he could use for competitive advantage. Prosecutors argue that the man's accomplices had authority to access the database for some purposes, but exceeded that authority when they accessed it for a purpose that violated corporate policy, which said that employees were only allowed to access the database to further the company's business interests. Unfortunately, a

[1] 18 U.S.C. § 1030(a)(2)(C).

[2] *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009); *See also* Electronic Frontier Foundation, *United States v. Drew*, <https://www.eff.org/cases/united-states-v-drew>.

[3] Electronic Frontier Foundation, *United States v. Lowson*, https://www.eff.org/cases/u-s-v-lowson.

federal appeals court initially ruled that an employee violates the CFAA when he uses a computer in way that violates an employer's restrictions; the court has decided to rehear the case, however, which is still pending.

If it stands, the *Nosal* decision is a dangerous precedent because it gives employers the power to make behavior criminal just by saying in a written policy that it is not allowed. For example, a worker could be sued or prosecuted for reading personal email or checking the score of a game if her employer's policy says that company computers may be used only for work.[4] The government might never choose to prosecute such trivial infractions, but it's important to remember that the CFAA is a civil statute, as well. Indeed, in *Lee v. PMSI, Inc.*, a company unsuccessfully argued that a former e12mployee violated the CFAA when she spent too much time checking personal email and browsing the Internet at work, which was prohibited by company policy. Fortunately, the court recognized the absurd implications of the former employer's sweeping argument and dismissed the claim.[5]

Companies have also tried to use the CFAA to stifle competition and maintain dominance in a given industry. In one ongoing case, *Facebook v. Power Ventures*, Facebook claims a start-up violated the CFAA and California state computer crime law by creating a service that allowed users to aggregate their information from a variety of social networking sites and view it in a single browser. Facebook has argued that Power violated the computer crime laws because it allowed users to access Facebook by automated means, which violated Facebook's Terms of Use. Facebook has also gone a step further, claiming that Power unlawfully designed its service to use multiple IP addresses to access Facebook's servers with the intention of defeating IP blocks. In other words, the mere creation of a tool that could be used to circumvent a technical barrier — even when a technical barrier doesn't exist — creates liability under the California Penal Code and the CFAA. This case shows that the companies can use the CFAA's imprecise language to stymie competitors who create new tools that would spur the economic market and give consumers more choices.[6]

---

[4] *United States v. Nosal,* 642 F.3d 781 (9th Cir. 2011), *rehearing en banc granted,* 661 F.3d 1180; *see also* Electronic Frontier Foundation, *United States v. Nosal,* https://www.eff.org/cases/u-s-v-nosal; Orin Kerr, N*inth Circuit Holds That Violating Any Employer Restriction on Computer Use 'Exceeds Authorized Access' (Making It a Federal Crime)*, Volokh Conspiracy (April 28, 2011), http://volokh.com/2011/04/28/ninth-circuit-holds-that-violating-any-employer-restriction-on-computer-use-exceeds-authorized-access-making-it-a-federal-crime/.

[5] *Lee v. PMSI, Inc.*, No. 8:10-cv-2904, 2011 U.S. Dist. LEXIS 52828 (M.D. Fla. May 6, 2011); *see also* Orin Kerr, Employer Sues Former Employee for Checking Facebook and Personal E-Mail and 'Excessive Internet Usage' at Work, Volokh Conspiracy (May 17, 2011), http://volokh.com/2011/05/17/employer-sues-former-employee-for-checking-facebook-and-personal-e-mail-and-excessive-internet-usage-at-work/.

[6] *Facebook, Inc., v. Power Ventures, Inc.*, No. 08-5780 JW, 2010 U.S. Dist. LEXIS 93517 (N.D. Cal. July 20, 2010); Electronic Frontier Foundation, Facebook v. Power Ventures, https://www.eff.org/cases/facebook-v-power-ventures.

These cases demonstrate that the government and private parties have argued with varying levels of success that the phrases ‘without authorization’ and ‘exceeding authorized access’ in the US CFAA should be broadly construed. The US experience can serve as a warning to European legislators that vague, ill-defined terms, especially concerning what computer access is 'authorized' or ‘exceeds authorization,’ can have deleterious effects for free expression, innovation and competition.

Mens Rea

The European Parliament should ensure that the draft Directive does not criminalize the legitimate activities and use of tools needed for independent security research, academic study, and other good-faith activities that serve the public interest and ultimately make the public more safe. The proposed text should affirmatively protect those activities, with a particular emphasis on protecting access for purposes of security testing. It is important to ensure that those activities or uses of tools without malicious *mens rea* are not punishable as criminal offenses. Examining computers without the explicit permission of the owner is necessary for a vast amount of useful research, which might never be done if permission were required.

As an initial matter, EFF suggests clarifying the definition of *mens rea* or criminal intent. The criminalization of conduct in **Articles 3 to 7** of the Draft Directive requires only that the perpetrator does not have a right to engage in certain behavior. Indeed, not having a right to engage in this behavior is not the same thing as — and is indeed broader than — having an malicious intent or *mens rea*, as is often required in criminal law, and instead turns general behaviors into strict liability crimes.

The recital to the proposed directive stipulates that when there is no 'criminal intent' then there is no crime, and lists examples of such scenarios including instances where there is authorized testing or protection of information systems. However, the recital does specifically allow access in circumstances where the perpetrator does not have the requisite *mens rea*, for example an 'unofficial' / 'unauthorized' test of the system's security in order to establish whether there are any vulnerabilities. The current formulation requires clarification especially to deal with legitimate behavior that is considered socially desirable such as the use of attack software in research and security testing.

The criminalization 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. It 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 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 CFAA by delivering information to conference attendees that it claimed could be used to defraud

the MBTA of transit fares. While a judge ultimately found that the presentation would not have violated the law, the MBTA's baseless lawsuit prevented the students from presenting their research at the conference, infringing their free expression rights.[7]

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 automated teller machines and program them to dispense money. Given the widespread use of bank accounts 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, the ATM flaws were secret for an entire year after Jack first intended to make their existence publicly known.[8]

Similarly, last year Sony sued researchers who disclosed security vulnerabilities in the Sony Playstation 3, including several who presented their research at the 2010 Chaos Communication Congress in Berlin. The flaws allowed users to install and run the Linux operating system on their PS3s — an option Sony once openly supported, but later took steps to prevent. Among other things, Sony made an overreaching argument under the CFAA that the researchers accessed their own video game consoles in a way that violated the agreement that Sony imposes on users of its network, despite the fact that the researchers didn't seem to have used Sony's network in their research — only the consoles they legally purchased. Simply put, Sony claimed it was illegal for the researchers to access their own computers in a way Sony didn't approve of. The case ultimately settled.[9]

There is a robust research community in Europe testing the security of computer systems to expose weaknesses in information systems now used in everyday life so that they can be improved.

---

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

[8] Kim Zetter, *ATM Vendor Halts Researcher's Talk on Vulnerability*, Wired.com (June 30, 2009), <http://www.wired.com/threatlevel/2009/06/atm-vendor-halts-talk/>; Kim Zetter, *Researcher Demonstrates ATM 'Jackpotting' at Black Hat Conference,* Wired.com (July 28, 2010), http://www.wired.com/threatlevel/2010/07/atms-jackpotted.

[9] Corynne McSherry and Marcia Hofmann, *Sony v. Hotz: Sony Sends a Dangerous Message to Researchers — and Its Customers,* Electronic Frontier Foundation (Jan. 19, 2011), <https://www.eff.org/deeplinks/2011/01/sony-v-hotz-sony-sends-dangerous-message>.

As the Chaos Computer Club in Germany explained: "Just as the automotive industry makes its automobiles safer with crash tests, in the computing field the security of systems is tested with the controlled use of attack programs."[10]

Two important examples of European researchers studying security flaws include Karsten Nohl, who in 2010 demonstrated how easy it was to eavesdrop on GSM-based mobile phones,[11] and academics at Ruhr University who in 2012 break two encryption systems used to protect satellite phone signals—and stated that the fact the encryption algorithms were secret meant that security experts could not test them.[12]

There have been legal actions against such security researchers in Europe. For example, in 2008, a court in the Netherlands ruled that Dr B. Jacobs Radboud at the University of Nijmegen was entitled to publish a scientific paper on security flaws in a wireless smart card chip. The chip's owner, NXP Semiconductors, argued that it would have been irresponsible to make this information public, but the court ruled that refusing to allow this article to be published would have violated the scientist's freedom of expression rights.[13]

Just last year, an independent researcher who found a vulnerability in German software firm Magix AG's music software and reported the flaw to the company was threatened with legal action when he wanted to publish information about the flaw after it was patched.[14] Similarly, German researcher Thomas Roth was served with an injunction in response to his plans to release an open source 'hacking tool' when a German newspaper mis-translated English-language news reports on his research, incorrectly reporting that he would be making a profit from hacking.[15] In the end, he managed to sort out the misunderstanding, but he was delayed in releasing his tool. Both of these cases involved the allegation that the researchers had acted contrary to the 'hacker paragraph' provision on German law, which criminalizes hacking tools (and is discussed more below).

---

[10] Chaos Computer Club, Prohibition of computer security tools opens the floodgates for the federal trojan- German statement, (Nov. 5, 2011), http://www.ccc.de/updates/2007/paragraph-202c

[11] Elinor Mills, Q&A: Researcher Karsten Nohl on mobile eavesdropping, CNET (Jan. 1, 2010), http://news.cnet.com/8301-27080_3-10423219-245.html.

[12] Christopher Williams, Satellite phone encryption cracked, The Telegraph (Feb. 3, 2012),http://www.telegraph.co.uk/technology/news/9058529/Satellite-phone-encryption-cracked.htm

[13] Elinor Mills, Dutch court allows publication of Mifare security hole research, CNET, (July 18, 2008),http://news.cnet.com/8301-1009_3-9994120-83.html.

[14] Kelly Jackson Higgins, Another Researcher Hit With Threat Of German Anti-Hacking Law, Security Dark Reading, (April 27, 2011),http://www.darkreading.com/vulnerability-management/167901026/security/vulnerabilities/229402356/another-researcher-hit-with-threat-of-german-anti-hacking-law.html.

[15] Kelly Jackson Higgins, Researcher Overcomes Legal Setback Over 'Cloud Cracking Suite', Secuirty Dark Reading, March 21, 2011, http://www.darkreading.com/authentication/167901072/security/client-security/229301362/researcher-overcomes-legal-setback-over-cloud-cracking-suite.html.

Austrian researcher Peter Kleissner has also faced legal action for exposing security weaknesses in Microsoft's Windows operating system. After Kleissner presented its research at the 2008 Black Hat conference, a prosecutor moved to build a case against him for violating Austrian anti-hacking laws.[16]

Indeed, there can be very important democratic interests in having access to systems to test for security vulnerabilities even when 'authorization' to do so is refused. In India, Hari Prasad, a computer scientist, was arrested in 2010 for refusing to disclose an anonymous source who provided an electronic voting machine to a team of security researchers. Prasad and his team had long questioned the security of the voting machines but the Indian government had refused to provide them with a machine to test, despite claims about election irregularities and fraud.[17]

As these examples demonstrate, independent researchers around the world working to improve security have faced legal threats under existing laws, despite the fact they have no malicious intentions and are performing work that ultimately serves the public. The draft directive threatens to make this problem worse and chill this important research in the future.

No Criminalization of Tools

We believe that **Article 7** regarding "tools uses for committing offences" should be eliminated. The current draft will severely curtail academic scholarship, legitimate security research, and other activities that benefit society.

As an initial matter, **Article 7** of the draft directive is largely duplicity of **Article 6** of the Convention on Cybercrime, which EFF opposed at the time of passage and continues to believe is troublesome.

Furthermore, the creation, possession or distribution of security tools shouldn't be criminalized *per se* under the proposed Directive because such tools are not inherently bad, but rather can be used for good and bad purposes. A classic example is a packet sniffer like Wireshark,[18] which could be used both for illegal wiretapping and for helping network administrators debug network configuration problems and identifying software bugs. The development and use of these tools are necessary for research and testing, including for "defensive" security efforts to determine the feasibility of attacks on a system.

---

[16] Sean Gallagher, Security Researcher Gets Root on Windows 8 with Bootkit, <http://arstechnica.com/business/news/2011/11/security-researcher-defeats-windows-8-secure-boot.ars>.

[17] Marcia Hofmann, *Security Researcher Arrested For Refusing to Disclose Anonymous Source,* Electronic Frontier Foundation (Aug. 23, 2010), https://www.eff.org/deeplinks/2010/08/security-researcher-arrested-refusing-disclose.

[18] Marcia Hofmann, *2011 in Review: Hacking Law*, Electronic Frontier Foundation (December 30, 2011), <https://www.eff.org/deeplinks/2011/12/2011-review-hacking-law>.

For example, a bank may hire a security consultancy to probe the bank's systems and report on vulnerabilities that need to be fixed. Since these tests are carried out with the bank's authorization, they are not a violation of the law, but they require the use of tools and techniques equivalent to those used by malicious attackers. Penetration testing — accessing a company's network with permission to detect security holes — is a growing security business, and security researchers will not be able to perform their jobs if the distribution of network utilities is criminalized.

The draft Directive should not criminalize the creation, possession and distribution of tools that are fundamentally designed for the purpose of carrying out an attack. These tools also can have legitimate, socially desirable uses, such as identifying a practical vulnerability. An example of software written essentially to carry out an attack or demonstrate a practical vulnerability is password-cracking programs such as Crack and John the Ripper. These tools are often used by system administrators to determine when users have chosen an insecure password that need to be changed. Academics and other researchers—who are studying password security—may also use them. Far from having criminal intent, these researchers use password-cracking programs to investigate how passwords might be made more secure.[19]

The current wording of the proposed directive may have a chilling effect on the production, development and use of tools in Europe which can be used to circumvent electronic censorship in authoritarian regimes—especially if these same tools could also have an 'illegal' use within the European Union. One example could be a system like Tor, which enables people to use the Internet anonymously by relaying their communications through a network of servers run by volunteers throughout the world. Internet users who run Tor relays may arguably be exhibiting 'criminal' conduct for the purposes of **Article 8** of the draft directive, which criminalizes the instigation, aiding and abetting of attacks on information systems contained in the previous articles. This would be a highly undesirable outcome, because online anonymity is important for many purposes, including the fact that it enables users to defeat censorship attempts by authoritarian regimes. Yet the draft directive does not discount this possibility.

---

[19] *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.

Article 7 does clarify that it permits 'dual use' tools whose *primary* purpose is the commission of offences in **Articles 3 to 6**. Yet this language is broader than the 2009 German Federal Constitutional Court's decision, which found that tools whose *only* purpose is to commit criminal acts were themselves criminal, interpreting a 2007 statute, known colloquially as the 'hackerparagraf' or s202c of the German Criminal Code, which criminalizes the 'preparation' of the interception of data.[20] Furthermore, the German Federal Constitutional Court emphasized the *intention* of the perpetrator was key in determining the criminality of the acts, a factor which seems to be absent from this proposed directive (for more on intent and *mens rea*, see the section above).

In any event, the 2007 German law was highly contested by groups such as the Chaos Computer Club and criticized for its vague language, which criminalizes the procurement and distribution of codes to access protected data as well as the production and use of tools that are useful for this purpose. The Chaos Computer Club also noted that since the coming into force of the law, there had been a decrease in the voluntary publication of detected security problems in Germany. They argued that the law would have the overall effect of lowering the standard of systems security in Germany.[21]

EFF also opposes this provision of German criminal law as over-criminalizing behavior, including that which can actually be socially useful—even though it is narrower than what is currently being proposed in the draft directive.

The amendments provided by the Rapporteur Monika Hohlmeier to remove mere 'possession' of such tools from the ambit of criminal liability should be adopted, although the recommendation to add 'clearly' still creates uncertainty as to what a 'clear aim' at committing one of the offences precisely means, and also is still broader than the 'primary purpose' adopted by the German Federal Constitutional Court.

The current state of affairs in other Member States such as the United Kingdom is that the conduct contained in **Article 7** is not criminal, and EFF believes this is the right result. If some form of **Article 7** should be retained, however, it should have a greater focus on criminal intent rather than mere creation, possession, or distribution of tools that can be used for good as well as malicious purposes. The Greens/EFA amendment seems to favor the German Court's position in advocating that only tools 'exclusively designed' for committing these offences be criminalized. In any event, even with a clarification on intent, this article remains very vague, with the potential to over-criminalize useful conduct.

EFF suggests that **Article 8** be deleted for many of the same reasons outlined above. The provision's wording is vague and does not protect intermediaries that do not have knowledge of

[20] BVerfG, 2 BvR 2233/07 of 05.18.2009, paragraph no. (1-77), <http://www.bverfg.de/entscheidungen/rk20090518_2bvr223307.html> (in German).

[21] Chaos Computer Club, Clause 202c of German penal code endangers German IT industry (Jul. 21, 2008), <http://www.ccc.de/en/updates/2008/stellungnahme202c>.

conduct that occurs through their systems. Furthermore, **Article 8** could criminalize 'whistleblowers' that publish information about system vulnerabilities. Moreover, the different meanings of 'instigating' in different Member States should be addressed.

The introduction of liability for systems owners and vendors in the new **Article 11** that the Greens/EFA propose certainly creates incentives for these entities to protect their systems better, and may be welcomed as creating efficiencies rather than providing no discouragement for these entities to do anything more than the minimum necessary to keep their systems operating.

We also believe that when the failure to protect data results in the unauthorized disclosure of personally identifiable data, vendors should be responsible for notifying the affected individuals and taking remedial steps to protect their rights.

Cloud Computing

We do not believe the Rapporteurs' Amendment to **Recital 9** to include cloud computing is necessary. The Convention on Cybercrime already addresses illegal computer access (**Article 2**), data interference (**Article 4**), interference with computer systems (**Article 5**), misuse of devices (**Article 6**), and computer-related fraud (**Article 8**), among other things. Cloud computing services are computer systems, and do not present unique or special concerns to justify greater law enforcement powers. We believe the Convention on Cybercrime is already highly problematic, and introducing additional, unnecessary regulation will only create additional concerns.

Rule of law

There are potential rule-of-law issues regarding the fact that public bodies are currently exempted from being held liable under this Directive if they break into computer systems without the right to do so, and also the proposal from the parliamentary committee to allow (private) service providers to shut down (allegedly) illegal systems or functions (in the absence of e.g. a court order declaring these systems/functions illegal), although the provision does claim that this will be done in accordance with the rule of law (yet with no specific information about how this will be achieved). Clarification of the steps that should be taken in order to preserve the rule of law here is highly necessary.

Summary of EFF's concerns on the proposed directive

In sum, we urge the European Parliament to make submissions on the following issues:

- We believe the Commission has not made a strong case for the necessity of this directive, especially given the existence of the Council of Europe Cybercrime Convention, which has not been implemented by all of the signatory states. Indeed, only 15 out of 27 Member States have ratified the Treaty (which EFF did not agree with at the time of its passage, since we believe it is overly restrictive).

- Aside from the fact that there is already legislative protection against computer crime in Europe, the lack of implementation of the Convention does not bode well for an effective enforcement of the proposed directive.
- We strongly urge that Article 7 on hacking tools be deleted entirely from the proposed directive. Its wording is vague and it would apparently over-criminalize behavior which would be considered socially beneficial such as the use of common security tools in research and testing.
- We oppose the more restrictively worded 'Hackerparagraf' of the German criminal code.
- The criminalization of security tools could chill important security research and allow vendors to deny the existence of flaws in their products, which could have socially detrimental effects if Article 7 is to be retained. The prohibition against 'possession' of tools should be removed too.
- A very precise definition should be sought of 'authorization' in Article 3, especially in light of the US experience with CFAA.
- There must be more clarification of what 'without right' means in Articles 3 to 7, and the role of *mens rea*/intent in establishing criminal liability.
- We support the deletion of **Article 8** regarding liability of *inter alia* intermediaries, and we would like to see a clarification of the protection of researchers and whistleblowers.
- We support the addition of **Article 11** to provide incentives for systems owners and vendors to protect their systems.
- We seek clarification as to how the rule-of-law issues regarding the conduct of public bodies and the possible inclusion of a provision allowing private service providers to shut down illegal systems and functions will be resolved.