Cite as Hidvégi & Zágoni, 8 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2016)

How Technology Enhances the Right to Privacy – A Case Study on the Right to Hide Project of the Hungarian Civil Liberties Union

Fanny Hidvégi[*] *& Rita Zágoni*[**]

INTRODUCTION

The Right to Hide project of the Hungarian Civil Liberties Union (HCLU) is a website dedicated to the promotion of privacy-enhancing technologies. The HCLU developed the www.righttohide.com (and in Hungarian the www.nopara.org) websites to offer tips and tools for every Internet user on how to protect their online privacy. Part I presents the legal and political atmosphere in which the HCLU realized the urgency to develop the www.righttohide.com website and discusses the current shortcomings of the Hungarian privacy, surveillance, and whistle-blower protection laws.

In Part II, we cover some of the theoretical and practical answers the website offers to these problems. We share these solutions through the HCLU's Right to Hide website as a way of surmounting the legal and political hurdles that limit the fundamental right to privacy in Hungary.

The HCLU is a non-profit human rights watchdog NGO that was established in Budapest, Hungary in 1994. The HCLU works independently of political parties, the state or any of its institutions. The HCLU's aim is to promote the cause of fundamental rights. Generally, it has the goal of building and strengthening civil society and the rule of law in Hungary and in the Central and Eastern European (CEE) region. Since the HCLU is an independent non-profit organization, it relies mostly on foundations and private donations for financial support. The HCLU strives to educate citizens about their basic human rights and freedoms through public education programs, and takes a stand against undue interference and misuse of power by those in positions of authority. The HCLU's Data Protection and Freedom of Information Program has been involved in a number of landmark privacy and access to information cases in Hungary and before the European Court of Human Rights. The HCLU also provides legal representation to whistle-blowers.

---

[*] Fanny Hidvégi has been the Head of Freedom of Information and Data Protection Program of the Hungarian Civil Liberties Union since 2012. Currently on sabbatical and works as International Privacy Fellow at the Electronic Privacy Information Center in Washington, DC.

[**] Rita Zágoni is the Head of Data Protection Program of the Hungarian Civil Liberties Union. With a background in programming, she focuses on the technological aspect of digital privacy protection.

Domestic human rights violations have been a primary focus of the HCLU; its mission is to protect the rights of individuals when the state abuses its powers. The HCLU's Data Protection Program, however, has broadened the scope of the program's activity to the private sector, to the special role of telephone and Internet service providers in particular. Yet, because there is a lack of adequate safeguards for the protection of personal data and the privacy of individuals, pursuing legal remedies in cases of privacy and other human rights violations can be difficult. Therefore, the HCLU has sought a solution that empowers average citizens and special groups like activists, journalists and whistle-blowers to proactively protect themselves. Strengthening the organization's capacities with a technologist was a key step in this direction. In February 2015, a team of lawyers, technologists, and communications experts started to work on the development of the HCLU's website to promote privacy enhancing technologies.

I. BACKGROUND: THE HUNGARIAN LEGAL AND POLITICAL ATMOSPHERE AND WHY THE RIGHT TO HIDE PROJECT WAS BORN

The driving force behind the Right to Hide project is a mixture of the following factors. We believe that the Hungarian legal regime (1) fails to provide adequate privacy safeguards (2) against the government's increasing surveillance laws and practices. The legal failure is complemented by (3) a lack of awareness and information among the citizenry. Based on our experience in human rights advocacy and legal aid, there is a pressing need in Hungarian society for a deeper understanding and appreciation of the value of human rights and the rule of law – privacy and data protection are hardly exceptions to the general lack of awareness. On top of that, the current political regime has (4) curtailed fundamental rights and undermined the rule of law and (5) taken antagonistic measures against its critics, including civil society organizations, journalists and whistle-blowers.[1] These groups have a compelling need for special online privacy protection. As noted on the HCLU website,

> In the past few years, the rule of law, democracy, pluralism, human rights and the role of independent institutions as checks and balances on political power have been

[1] *Actions that Undermine the Values and Principles of OGP in Hungary: A Chronology of Attacks on Civil Society*, OPEN GOVERNMENT PARTNERSHIP (June 2016), http://www.opengovpartnership.org/sites/default/files/attachments/OGP%20Hungary%20response%20policy%20background%20document.pdf.

> systematically undermined in Hungary. Particularly troublesome are the government's actions to reduce the space for nongovernmental organizations to work independently, voice critiques and receive funding from international sources. Since the summer of 2013, Hungarian government officials have been engaging in a smear campaign against some of the country's independent NGOs [including applying administrative sanctions and carrying out police raids].[2]

The primary goals of the Right to Hide project are to educate, empower and raise awareness by offering hands-on tools and tips to increase the level of online privacy and data protection for all people - either members of a special target group or just average Internet users.

Generally speaking, the revelations by Edward Snowden have changed the debate about privacy advocacy in recent years; yet, this effect was not as strong in Hungary as in other European countries, Germany, in particular. It is a telling story that while the surveillance and hacking of Chancellor Merkel's phone made headlines and became part of international negotiations and politics, Hungary's Prime Minister Viktor Orban reacted by saying that he never uses his cell phone for sensitive matters. Instead he "strolls" to someone to talk.[3] Furthermore, before the *Schrems* case made headlines in Europe,[4] spying on US citizens received more coverage, and prompted more intense legal debate, than the surveillance of non-US citizens. As a consequence, the level of engagement of the Hungarian press cannot be compared to the level of their American counterparts.

It does not help that most existing websites that promote privacy-enhancing technologies are in English and thus less accessible to non-English speakers.[5] The Right to Hide website, however, is written in Hungarian and has an English version as well. As such, the HCLU believes that the site will add value to the international community; yet, the primary focus is to create a digital privacy hub for Hungarians. We aim to engage a general audience by building on our prior work with journalists and whistle-blowers and offer them special solutions tailored to their situations.

A. Lack of Adequate Safeguards in the Legal Framework of Privacy and Surveillance

[2] *HCLU called OGP to investigate the situation in Hungary*, HUNGARIAN C.L. UNION (July 9, 2015), http://tasz.hu/en/freedom-information/hclu-called-ogp-investigate-situation-hungary.
[3] Péter Magyari, *Orbán: Odabattyogok, nem telefonálok*, 444 (Oct. 25, 2013), http://444.hu/2013/10/25/orban-odabattyogok-nem-telefonalok.
[4] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 ECLI:EU:C:2015:650 (Oct. 6, 2015).
[5] *See, e.g.*, SURVEILLANCE SELF-DEFENSE, ELECTRONIC FRONTIER FOUNDATION, https://ssd.eff.org (2014).

As the Right to Hide project is primarily aimed at average Internet users, thus a general audience, the website strives to present safeguards to government surveillance that are of use to every Hungarian citizen. To be adequate, privacy safeguards require a minimum standard for redress mechanisms, transparency, and oversight. None of these are met by the Hungarian legal framework and its implementation. As noted on the HCLU's website, "National legislation governing surveillance is inadequate, leaving significant regulatory gaps and providing weak safeguards, oversight and remedies against unlawful interference with the right to privacy, including in relation to data retention provisions and the lack of judicial authorization and oversight of the surveillance conducted for purposes of national security."[6]

Article 6 of the Hungarian Fundamental law recognizes the right to privacy (paragraph 1)[7] and the right to protection of personal data (paragraph 2.)[8]. The means by which these fundamental rights are affected are laid down by the Act CXII of 2011 on Informational Self-determination and Freedom of Information.[9] Nonetheless, there are many sectoral laws affecting the rights to privacy and protection of personal data.

The following overview of the legal framework related to government surveillance is based on the joint report of the HCLU and Privacy International[10] submitted to the UN Human Rights Council. It also covers the most recent Hungarian developments related to encryption and surveillance.

1. Inadequate Authorization and Oversight of Surveillance for the Purpose of National Security

There are two types of intelligence surveillance powers in Hungary: secret surveillance for the purposes of criminal investigation, and secret surveillance for the purposes of national security. The HCLU's main concerns relate to surveillance for the purposes of national security, from which judicial authorization and oversight are effectively absent.

---

[6] *Aggályos megfigyelési gyakorlatok*, HUNGARIAN C.L. UNION (Sept. 7, 2015), http://tasz.hu/adatvedelem/aggalyos-megfigyelesi-gyakorlatok.
[7] MAGYARORSZÁG ALAPTÖRVÉNYE [THE FUNDAMENTAL LAW OF HUNGARY], ALAPTÖRVÉNY VI. CIKK (1) BEKEZDÉS [ART. VI, ¶ 1].
[8] MAGYARORSZÁG ALAPTÖRVÉNYE [THE FUNDAMENTAL LAW OF HUNGARY], ALAPTÖRVÉNY VI. CIKK (2) BEKEZDÉS [ART. VI, ¶ 2].
[9] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Act CXII of 2011 on Informational Self-Determination and Freedom of Information) (Hung.).
[10] *Aggályos megfigyelési gyakorlatok*, *supra* note 5.

For the purpose of national security, Act 125 of 1995 of the National Security Services[11] primarily allows the "National Security Services" to carry out secret surveillance. The National Security Services are four agencies set up by the law with different duties. According to Act XXXIV of 1994 on the Police,[12] the Counter Terrorism Center – a separate part of the Hungarian police – is also allowed to use secret surveillance methods for criminal and non-criminal investigatory purposes. These forms of intelligence gathering include but are not limited to searching residences in secret and recording observations with technical devices; tracking communication through a public telephone line or some other telecommunication service; and tracking, recording, and using data transferred or stored on IT devices or system.

Unlike the gathering of intelligence for criminal investigation purposes, there is no requirement for prior judicial authorization of surveillance for purposes of national security by the Counter Terrorism Center and in some cases by the National Security Services. Instead, the Minister of Justice provides the authorization. The Minister's decision is not subject to appeal. What's more, the person who is subject to surveillance has no right to be informed about the decision, as the Minister of Justice need not inform the party concerned of his proceedings or of the fact of intelligence gathering. The case *Szabó and Vissy v. Hungary* challenged this legislation, claiming that this lack of judicial authorization violated the Hungarian Constitution. The Hungarian Constitutional Court disagreed, ruling that it did not.

Following this judgment,[13] the petitioners turned to the European Court of Human Rights.[14] As potential subjects of surveillance, they claimed that their rights to privacy are violated if the interception lacks a control mechanism independent from the government and surveillance-gathering parties. This is especially true because, given the secret nature of this type of surveillance, concerned persons are usually unaware of the fact that they are being watched, and are therefore unable to enforce

[11] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról (Act CXXV of 1995 on the National Security Services) (Hung.).
[12] 1994. évi XXXIV. törvény a Rendőrségről (Act XXXIV of 1994 on the Police) (Hung.).
[13] Alkotmánybíróság (AB) [Constitutional Court] Nov. 18, 2013, AK.IV/03085/2012 (Hung.).
[14] In a case against Hungary before the European Court of Human Rights, Szabó v. Hungary, App. No. 37138/14, HUDOC (Eur. Ct. H.R. Jan. 12, 2016), http://hudoc.echr.coe.int/eng?i=001-160020, the petitioners alleged that the power to collect intelligence information upon citizens based on a simple ministerial authorization but without a court warrant violates their rights under Article 8 of the European Convention on Human Rights. *See Szabo and Vissy v. Hungary*, EÖTVÖS KÁROLY POL'Y INST., http://www.i-m.mx/szabomat/SzaboAndVissyVHungary.

the rights protecting them from such activities.[15]

The European Court of Human Rights in *Szabó and Vissy v. Hungary*[16] declared once and for all that uncontrolled government surveillance is incompatible with European human rights standards including the European Convention on Human Rights. The court's decision means that, instead of mass, indiscriminate data gathering, Hungarian authorities must obtain a judicial warrant to collect data on a case-by-case basis. The judgment has all the more weight since the decision was clearly not influenced by the terror threat in Europe, reinforcing the concept that judicial rulings should set the standards for government behavior, with only limited exceptions being allowed in extraordinary circumstances.[17]

This case was not the only one in which the Hungarian Constitutional Court failed to fulfill its obligation to protect and ensure fundamental rights. Another striking example involves the Court's response to the government's Data Retention Directive, which calls for mandatory data retention by Internet and telephone service providers.[18]

Internet and telephone service providers have a key role in digital surveillance as intermediaries between the citizens and the government. In April 2014 the Court of Justice of the European Union (CJEU) declared invalid the retention of communication data by Internet and telephone service providers under the Data Retention Directive.[19] Despite the CJEU's ruling, however, the Hungarian Act remained in force.[20] Thus, the HCLU initiated litigation, seeking a judgment from the Hungarian Constitutional Court to repeal this provision. Regrettably, when the Constitutional Court took up the case (on request from the ordinary court before which the case was heard[21]), the Constitutional Court

---

[15] *Judicial Warrants are Required for Government Surveillance*, HUNGARIAN C.L. UNION (Jan. 15, 2016), http://tasz.hu/en/data-protection/judicial-warrants-are-required-government-surveillance.
[16] *Szabó v. Hungary*, *supra* note 13.
[17] *Judicial Warrants are Required for Government Surveillance*, *supra* note 16. The ECtHR in its decision has built on previous jurisprudence such as the judgment in the *Zakharov* case concerning the Russian legal provisions governing communications surveillance that did not provide enough safeguards against mismanagements in the use of the system, such as arbitrariness or abuse. *See* Zakharov v. Russia, App. No. 4713/06, HUDOC (Eur. Ct. H.R. Dec. 4, 2015), http://hudoc.echr.coe.int/eng?i=001-159324.
[18] *Hungary's Government Has Taken Control of the Constitutional Court*, HUNGARIAN C.L. UNION (Mar. 24, 2015), http://tasz.hu/en/rule-law/hungarys-government-has-taken-control-constitutional-court.
[19] According to the decision, the directive had exceeded the limits of proportionality concerning the right to privacy and protection of personal data, as it failed to establish guarantees that counterweigh such limitations. Case C-293/12, Dig. Rights Ireland v. Minister for Commc'ns, Marine and Nat. Res., 2014 ECLI:EU:C:2014:238 ¶ 69 (Apr. 8, 2014).
[20] *The never ending data retention*, HUNGARIAN C.L. UNION (June 22, 2015), http://tasz.hu/node/16417.
[21] Due to the reform of the jurisdiction of the Constitutional Court, HCLU could not directly refer the case to the Constitutional Court. Instead, it had to initiate a long process beginning litigation against Hungarian telephone and Internet service providers.

failed to rule on the merits of the case, arguing that the claim did not pertain to the retention of communication data. While this case is still pending, the Constitutional Court judgment constitutes a significant obstacle for individuals and organizations to obtain an effective remedy for this interference with their right to privacy. The judgment also goes against trends in other EU member states, where courts have declared that domestic data retention legislation is incompatible with the right to privacy and the right to personal data as provided for in the European legislation.[22]

The inadequate authorization of surveillance powers is accompanied by ineffective oversight mechanisms. Parliamentary oversight of the National Security Services is conducted by the National Security Committee.[23] The chair of the National Security Committee is always a member of the parliamentary opposition. The Committee has powers to exercise parliamentary control through, inter alia, measures including but not limited to requesting information from Ministers and from the general directors of the National Security Services, and investigating complaints of unlawful activity by the National Security Services. Despite its relatively strong power, this parliamentary control is considered political and not easily accessible to average citizens. According to our information, these procedures have never been triggered.

In theory, the activities of the National Security Services are not excluded from the application of the general data protection act, Act CXII of 2011 on Informational Self-Determination and Freedom of Information. Therefore data protection remedies and redress mechanisms are applicable, including investigation by the National Data Protection and Freedom of Information Authority (DPA).[24] The Hungarian DPA was established on January 1, 2012 by prematurely terminating the mandate of the former Data Protection Commissioner. However, the Act on National Security Services provides for exemptions under these remedies.[25] Moreover, there are serious concerns about the independence of the DPA following the circumstances of its establishment[26] and its activities.

---

[22] For example, the July 2015 judgment of the UK High Court declares parts of the Data Retention and Investigatory Powers Act 2014 (DRIPA) to be in violation of the right to privacy and the protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The Queen v. Sec'y of State for the Home Dep't [2015] EWHC (Admin) 2092 [114].
[23] For the Military National Security Service, the oversight is in co-operation with the Committee for Defense and Law Enforcement, although it is the National Security Committee that is responsible for the parliamentary control over the Military National Service's classified activities.
[24] European Commission Press Release, Court of Justice upholds independence of data protection authorities in case against Hungary (Apr. 8, 2014).
[25] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, 48. § 1 (Act CXXV of 1995 on the National Security Services) (Hung.).
[26] *The Hungarian data protection authority was conceived in sin*, HUNGARIAN C.L. UNION (Apr. 10, 2014), http://tasz.hu/node/4113.

The Commissioner for Fundamental Rights also has power to investigate complaints related to secret surveillance. Despite his powers, the Commissioner has never conducted any investigation on secret surveillance or other privacy matters since the establishment of the DPA.

As a consequence, the level of authorization limitations and oversight is weak, and the legal framework does not provide adequate safeguards against unlawful surveillance.

2. Unlawful Surveillance Practices

The inadequacies of the legal framework related to privacy safeguards and surveillance laws create a violation of the fundamental rights to privacy and data protection. To more thoroughly explain the factors that created the need for the Right to Hide project, we should also discuss the implementation of these laws and emerging surveillance practices.

a. Introduction of CCTV Cameras with Facial Recognition Capability

During the 2014 national election campaign, the mayor of District 8 in Budapest launched a project costing 250 million Hungarian forints (HUF) (approximately 1 million USD) to set up 70 new closed-circuit televisions (CCTVs) with facial recognition capabilities.[27] According to the local government, the additional 70 cameras provide full coverage of the district.[28] Note, however, that there is no law that provides a legal basis for collecting and processing such data. Furthermore, while the cameras were purchased by the local government, the authority responsible for processing the data is the Special Service for National Security – one of Hungary's national security agencies.[29] Consequently, every detail concerning the capabilities of the cameras and the data processing (including the time of retention and persons with access to the footage) is confidential and lacks transparency.

The project included a "social consultation" campaign in which the local government sent

[27] Somogyi Dorottya, *Arcfelismerő kamerák a Józsefvárosban: lesz képük hozzá?*, VS (Aug. 7, 2014), http://vs.hu/kozelet/osszes/arcfelismero-kamerak-a-jozsefvarosban-lesz-kepuk-hozza-0807.
[28] *Mindenhol lesznek terfigyelő kamerák*, JÓZSEFVÁROS ÖNKORMANYZAT HONLAPJA (June 30, 2014), http://jozsefvaros.hu/hir/1918/mindenhol_lesznek_terfigyelo_kamerak.
[29] *Cf. Task of directorates laid down by law*, SPECIAL SERV. FOR NAT'L SECURITY, http://www.nbsz.gov.hu/?mid=28.

letters to inhabitants of the district to ask for proposals about the location of the new cameras. However, the whole process remains shrouded in secrecy: although the purchase was covered by public money, every Freedom of Information request regarding the public procurement or the cameras has been denied by the local government on the basis that this information is classified.

Besides the obvious and very serious interference with the right to privacy and the right to data protection, the installation of CCTV cameras in a neighborhood with a high Roma population may facilitate the discriminatory practice of the Hungarian police against Roma people.[30]

Moreover, under recently enacted legislation,[31] a searchable registry of pictures of every Hungarian citizen will be operational by the end of 2016. The Special Service for National Security would have broad authority to request data from that registry, giving it the capacity to make secret, remote, and bulk identifications of citizens.

b. Network Exploitation

Because of the secrecy surrounding state surveillance, the full range of digital surveillance techniques employed by the security services in Hungary is unknown. However, there are reports that sophisticated malware marketed by the Italian and German companies Hacking Team and Gamma International is currently or has previously been in use by security services in Hungary.[32] There appears to be no explicit legislative authority in Hungary for the National Security Services to use such technologies that are capable of hijacking computer and mobile devices, whilst remaining undetectable to users.[33]

c. Most Recent Developments

On top of the above described legal and implementation-related infringements, the latest

[30] *A Hungarian City Openly Against Its Roma*, HUNGARIAN C.L. UNION (July 14, 2015), http://tasz.hu/en/romaprogram/hungarian-city-openly-against-its-roma.
[31] 2015. évi CLXXXVIII. törvény az arcképelemzési nyilvántartásról és az arcképelemző rendszerről (Act CLXXXVIII of 2015 on the Image Profile Registration and Analysis System) (Hung.).
[32] *The buzz about the business of government surveillance – after the Hacking Team hack*, EURONEWS (July 8, 2007), http://www.euronews.com/2015/07/08/the-buzz-about-the-business-of-government-surveillance-after-the-hacking-team.
[33] H4XXX0R, *Magyarország 600 milliót fizetett a világ legostobább hekkereinek*, INDEX (July 7, 2015), http://index.hu/tech/2015/07/07/600_milliot_fizettunk_a_vilag_legostobabb_hekkereinek (Hung.).

developments in Hungarian surveillance laws are extremely worrisome and contrary to human rights standards. First, the Hungarian government has been exploiting the European refugee crisis and terror attacks to introduce a new type of a state of emergency in relation to terror threats.[34] Second, after the Paris and Brussels terror attacks, the Hungarian government joined other European countries (and the Apple v. FBI debate) to undermine encryption and introduce new surveillance powers.[35] Government officials started to talk about these amendments without making the texts of the proposals public and prevented meaningful social and political debate on these issues.[36] The HCLU obtained and published a secret government proposal that would criminalize both providing and using any end-to-end encrypted software, application, or other service with two-year imprisonment.[37] According to government sources this part of the proposal is no longer on the table. And finally, the proposed "anti-terror" legislative package does not include the necessary amendment to comply with the judgment of the European Court of Human Rights in *Szabó v. Hungary*.

B. Lack of Effective Whistle-Blower Protection in Hungary

This paper gives special attention to the Hungarian whistle-blower law for two reasons. First, whistle-blower protection would be essential to counterbalance the government's excessive surveillance powers; therefore, the inadequacies in that legislation add to the problems described in Section II.1. And second, although the Right to Hide project aims to offer privacy protections for every Internet user, the HCLU's legal work has showed the need to raise awareness among people at higher risk, including journalists, activists, and whistle-blowers.

Alongside journalists and activists, whistle-blowers constitute a special target group for those in power; hence, whistle-blowers must make extra efforts to protect their safety and security. They cannot rely on the current legal framework, which fails to provide the necessary guarantees. Consequently, digital privacy plays a key role in whistle-blower protection. To better grasp the need for the privacy solutions we set forth later in this paper, it is useful to understand the Hungarian whistle-blower

[34] Chris Tomlinson, *Hungary Declares State of Emergency, Deploys Thousands of Troops to Border*, BREITBART (Mar. 10, 2016), http://www.breitbart.com/london/2016/03/10/hungary-declares-state-of-emergency-deploys-thousands-of-troops-to-border.
[35] *UK Home Office introduces fast-tracked, deeply flawed Investigatory Powers Bill*, ACCESS NOW (Mar. 1, 2016), https://www.accessnow.org/uk-home-office-introduces-fast-tracked-deeply-flawed-investigatory-powers-bill-2.
[36] *Hungarian government plans to enforce encryption backdoors*, HUNGARIAN C.L UNION (Apr. 1, 2016), http://tasz.hu/en/news/hungarian-government-plans-enforce-encryption-backdoors.
[37] The document and the HCLU's legal opinion are only available in Hungarian, http://tasz.hu/adatvedelem/tasz-allaspontja-terrorizmus-elleni-fellepessel-osszefuggo-egyes-torvenyek-modositasarol.

protection regime and the practical implementation of the law.[38]

1. Shortcomings of the Statute

A new whistle-blower act came into force on 1 January 2014 (Act CLXV of 2013 on Complaints and Public Interest Disclosures).[39] According to the law, whistle-blowing is defined as revealing a harmful practice or situation to the authorities when the correction or termination of that practice or situation would be beneficial for the community or the whole society. The law does not define the scope of protection with regard to the topic of the whistle-blower's report.

Procedurally, the 2014 law gave new power to the Office of the Commissioner for Fundamental Rights, to which whistle-blowers can report their complaints. Whistle-blowers can turn to the Office of the Commissioner for Fundamental Rights in person or electronically through a special online system. The HCLU recommends the electronic approach because it provides better protection for the whistle-blower's personal data. However, the Commissioner does not take the content of these reports into consideration but forwards them to the entity that is authorized to investigate and remedy the alleged violation. It then reviews the conduct of such investigations.

Instead of going to the Commissioner for Fundamental Rights, whistle-blowers also can go directly to the public authority that is authorized to take action in the case that is being reported. The Act does not make clear, however, whose responsibility it is to investigate whistle-blower reports within the authority. There is no best practice of who to turn to and the Act provides virtually no guidance besides referring to the authority entitled to proceed. The best solution in general might be for the whistle-blower to report to the person competent in public affairs within the competent authority. It is likely that the case would then be investigated by the organization's so-called integrity commissioner. Under the Act, government agencies must identify an integrity commissioner who is authorized to handle whistle-blower complaints.

According to the Ministry of Justice, which was previously responsible for developing this

[38] Our analysis is based on the joint report of HCLU and K-Monitor submitted to the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. The analysis includes the responses we received from the Ministry of Justice as to the interpretation of the law. *See Kiáll a közérdekű bejelentők védelméért a TASZ*, HUNGARIAN C.L. UNION (Sept. 7, 2015), http://tasz.hu/informacioszabadsag/kiall-kozerdeku-bejelentok-vedelmeert-tasz.
[39] 2013. évi CLXV. törvény a panaszokról és a közérdekű bejelentésekről (Act CLXV of 2013 on Complaints and Public Interest Disclosures) (Hung.).

legislation, the person responsible for dealing with complaints and whistle-blower reports is the head of the organization. This is clearly problematic when the corruption or other wrongdoing is connected to the management of that organization. No guarantees are implemented to support unbiased, professional and fair investigation. In the current system there is a high risk that reports are investigated by people/bodies that are subjects of the report.

By definition of the scope of the law, it fails to provide meaningful protection, as whistle-blowing is determined not as the disclosure of information but reporting a problem to the responsible authority and not to the public. Hence, whistle-blowers seeking to publish information disclosing wrongdoings are not protected under the act. What this means in practice is that whistle-blowers turning to the media or civil society organizations are not protected. They risk being dismissed from their places of work, and can even be prosecuted for a breach of confidentiality or charged with defamation. The whistle-blower protection regime also fails to provide for the right to respect for private and family life because the legislation does not offer any protection for family members. Although this may seem like an ambitious request, the lack of protection for family members makes whistle-blowers more vulnerable.

The most crucial provision of the law is the one stating that every measure detrimental to the whistle-blower taken as a result of the whistle-blower's report is unlawful even if it was legitimate otherwise.

When filing a report, whistle-blowers usually have to disclose confidential information. The law, however, does not explicitly release whistle-blowers from their obligation of keeping these secrets regardless of the topic of the report or nature of the confidentiality obligation. Without the waiver of such obligation the entire legal concept is senseless. The public interest of protecting business secrets ceases to exist if it is used to cover up criminal activity.

According to the Ministry of Justice the only secure way to blow the whistle is through the electronic system operated by the Commissioner for Fundamental Rights because the Office of the Commissioner for Fundamental Rights has authorization to manage confidential data. If the whistle-blower decides to lodge her report at the government agency authorized to evaluate the report (according to the whistle-blower), it creates an additional risk on the whistle-blower. If so doing, it will be the whistle-blower's responsibility to assess whether it is lawful if the certain government agency

becomes aware of the classified information in question. This legal and practical problem proves to be an unjustified burden on the whistle-blower.

Assuming that the Office of the Commissioner forwards the report of the whistle-blower to the agency entitled to investigate, the question is what happens if (a) the whistle-blower's report is not investigated properly or objectively, or (b) a detrimental measure is taken against the whistle-blower. In the first case, it is the duty of the Commissioner, without consideration of the content of the report, to inspect if the competent body has conducted the investigation fairly and lawfully. The law,[40] which defines the competencies of the Commissioner for Fundamental Rights, sets out that regarding the compliance of the investigations they conducted in certain cases reported by whistle-blowers, the Commissioner for Fundamental Rights can only inspect a closed circle of bodies (public authority, local government, law enforcement body etc.). The Commissioner for Fundamental Rights' website does not speak of such restrictions but of a possibility of revision in general. In the second case, there is no agency in the Hungarian public administration responsible for investigating whether a whistle-blower has suffered detrimental measures as a consequence of her report.[41] The law only provides a formal way to appeal, since the Office of the Commissioner for Fundamental Rights has neither the legal authority nor the capacities to conduct substantive investigations.

2. Shortcomings of the Practical Implementation of the Law

On top of the deficiencies of the legal regime on whistle-blower protection, the consequences of how the law is implemented in practice might turn out even more disadvantageously for whistle-blowers. On a personal level, the financial and psychological risks are among the primary dangers for whistle-blowers.

Theoretically, if a whistle-blower's report puts her living conditions at risk, she is eligible for whistle-blower-support. The government decree that would regulate the means of financial compensation has not been enacted since 2014. However, the current legislation provides limited general legal aid, free of charge, for the whistle-blower who can request this at government offices.

---

[40] 2011. évi CXI. törvény az alapvető jogok biztosáról (Act CXI of 2011 on the Commissioner for Fundamental Rights) (Hung.).

[41] *Konferencia az Ombudsmani Hivatalban: Félnek a bejelentők* [Meeting of the Ombudsman's Office: They are afraid of whistleblowers], BEVÉD, http://beved.hu/news/meg-egy-hir (Hung.).

Note that the current legislation does not reward the whistle-blower.[42]

According to the Ministry of Justice, at the moment of filing their report, whistle-blowers become protected. It is the responsibility of the opposing party to prove if the whistle-blower was malicious and provided false information. A report is considered malicious if it intentionally includes false information that has significant relevance in the case. Detrimental measures against a whistle-blower can only be justified if her misconduct is proven. However, in case of suspicion of wrongdoing, proceedings that aim to reveal a possible crime are not considered detrimental measures. This means that the protection guaranteed by the law does not prevail in practice. While the act suggests that when a report is filed, the whistle-blower is protected from any detrimental measure against her, it does not explicitly provide a defense for the disclosure of confidential information, nor from the opening of criminal proceedings against the whistle-blower. Criminal proceeding can be conducted in order to investigate whistle-blower's reports, but our point of view is that they can never be directed against the whistle-blowers themselves.

Anonymity is a key factor in the protection of whistle-blowers. Yet, the online whistle-blower report interface is deceptive with regard to the question of anonymity. It offers two options for filing a report. First, reports can be filed through an online government services portal (called Ügyfélkapu). This option raises serious concerns, though, as the whistle-blower cannot control what government agencies can access their report. The second option is "Lodging a whistle-blower's report without identification" which implies that the whistle-blower does not have to provide personal data for the identification.[43] This is not true in practice. The whistle-blower must provide a name and address. The whistle-blower, however, can request that only the Office of the Commissioner for Fundamental Rights can access their personal data. In this case, the Office of the Commissioner for Fundamental Rights will only forward the excerpt of the report to the competent authority. In the HCLU's point of view, the government should provide a truly anonymous reporting option.

Unsurprisingly, the legal and practical shortcomings of the system have resulted in the

[42] There is one exception, however: according to the Competition Law, whistle-blowers who provide indispensable evidence for the Hungarian Competition Authority for the investigation of cartels. Both the competition law and the penal code make it possible for the participants of criminal acts to be excused from punishment (or get a less severe sentence) if they take part in revealing the offence before the criminal investigation. 1996. évi LVII. törvény a tisztességtelen piaci magatartás és a versenykorlátozás tilalmáról (Act LVII of 1996 on Prohibition of Unfair and Restrictive Market Practices) (Hung.).

[43] It is actually translated as "Lodging a complaint" on the website, even though there is a difference between a whistle-blower's report and a complaint under the law.

government taking severe measures[44] against whistle-blowers in recent years.[45] For example, the HCLU has represented a former contractor of the Hungarian National Tax and Customs Administration, András Horváth, who went public with information about companies committing VAT fraud with the assistance of the National Tax and Customs Administration (NAV) only after trying unsuccessfully on several occasions to raise his concerns within the Administration itself and to the Government. As a consequence, the police raid his home and pressed charges against him.[46]

The main conclusion which can be drawn by the deficiencies of the legal regime and moreover, the implementation thereof, is that the current laws and practices do not provide sufficient protection to whistle-blowers, and have to be reshaped fundamentally. In the absence of adequate safeguards for whistle-blowers, human rights activists and journalists, the HCLU offers hands-on solutions for protecting their digital privacy as well as the privacy of average Internet users.

II. THE RIGHT TO HIDE: A TECHNOLOGICAL ANSWER

The Right to Hide project aims to give a technological answer to legal shortcomings by empowering whistle-blowers and activists to securely communicate in the face of potential surveillance. The goal of the website is to raise awareness about the importance of protecting privacy online, and to provide information, tools, and tips for using privacy-enhancing technologies for whistle-blowers and activists. However, we also aim to reach a broader audience of Internet users who have not yet dealt with the issues of online privacy.

The guiding principles of the site are as follows:

1. Equality: we will only promote free, open source tools because the fundamental right of privacy already suffers from inequality problems that should not be deepened: no one should have to pay for privacy.
2. Our target audience is the general public, but we provide solutions to special groups

[44] *Hungarian whistleblowing case unfolds*, WHISTLEBLOWING INT'L NETWORK (Apr. 7, 2014), http://whistleblowingnetwork.org/2014/04/07/hungarian-whistleblowing-case-unfolds.
[45] *See, e.g.*, *Why was the search of the whistleblower's home unlawful?*, HUNGARIAN C.L. UNION (Apr. 7, 2014), http://tasz.hu/en/freedom-information/why-was-search-whistleblowers-home-unlawful.
[46] The legally acceptable solution from the state would be to regard reports as bona fide until proven otherwise, just like the presumption of innocence. The state should not have the right to conduct criminal proceedings or carry out searches until it has ascertained the content of the report.

like human rights activists, journalists and whistle-blowers.

3. Everyone is responsible not only for creating a higher level privacy but also for maintaining it. It cannot be overemphasized that this job is never done. Therefore, we will indicate how up to date each tool is and we will work on the website continually to keep it current with the newest privacy-related technology.

4. We believe that this knowledge cannot come from one single organization. We have designed our site to foster a community that is constantly using these tools and communicating about them, with us and with each other, therefore contributing to the further development of the site.

Different uses of digital technologies pose different kinds of privacy risks. In this section we give an overview of the main types of risks and current technologies that are capable of addressing them, that is, that have the potential to provide more or less control over which data we share, how, and with whom. We will also showcase a selection of specific tools most of which will be presented on the site, indicating the potential target audience and users. Where applicable, future technological perspectives will also be noted.

In the next section, we divide digital technologies into four main categories based on the threats they pose as follows: (1) controlling access to online profiles; (2) communication by email/chat and communication with other devices in a network; (3) browsing behavior; and (4) storing data online.

A. Access

As access-related security measures are the first step towards a general information security, they are relevant for all audiences.

Data created by users during digital activities – digital traces, so to speak – come from a variety of sources ranging from browsing history to cell phone location data. Large portions of this data are available in complete packages as information linked to online accounts: a Facebook account contains personal messages, saved links and pages reflecting one's interests; public as well as private group memberships reveal preferences, together with birth date, work history and contact information; online shopping accounts store credit card information. If the user provides the same e-mail address for each account, the information can be tied together easily into a profile; similarly, a Google account

combined with a Chrome browser creates a comprehensive personal profile based on search and browsing history.

The first step to protecting privacy is to control access to accounts by some form of authentication. A password can provide security because it authenticates a user with something they, and only they know, as long as it cannot be inferred. Strong passwords that are long, complex, and unique – as is generally recommended – cannot be linked to the user, but storing them safely can be a challenge in everyday use.

What is more, passwords fail to provide a high level of protection because they afford only one layer of security: if a password is compromised, the account is instantly accessible. Therefore it is becoming widespread to add another layer of authentication and thus create a two-factor authentication. The additional layer consists of providing information from a device that users keep with themselves, typically a mobile phone, which they need to register with the service they want to use. The service then sends a one-time code to the device in order for the user to gain access. While this process increases security, it also raises privacy risks because it allows a direct link between one's online and offline identity through a range of services.

Single sign-on frameworks are part of another trend that allows for users to connect to different online services using a single online identity like a Google or Facebook account. This type of login makes it easier to track users' behavior through a range of services, even more so because these online identities are usually directly linked to users' offline ones.

Password management tools as Lastpass and Keepass offer a range security options: storing passwords encrypted in the cloud or on the hard drive, two-factor authentication for sign-in to the service, location-based sign-in allowing access from only certain locations, and generating secure passwords automatically.

Research is ongoing about the potential of attribute-based authentication that could serve as a more effective privacy-preserving means of access control.[47] In many cases, access to a service does not depend on a user's verifiable identity but on the user having a certain set of attributes, making it

[47] *See, e.g.*, Vipul Goyal et al., Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data, *in* PROCEEDINGS OF THE 13TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 89, 91 (2006).

unnecessary to reveal the user's identity. For example, in order to access paid media online, a user can be issued a certificate showing only that the user has signed up for the service, but not the user's identity. This way, her logins and media consumption on the side cannot be linked together or attached to her identity. The main advantage is that users can use different attributes as keys to different services, thus, as opposed to using an email address as a username or single sign-on, the services used cannot be linked to their user, and each identity can be kept separate from the others.

B. Communication

In this section, we will look at ways of protecting two forms of online communication: 1) the content of communication through email and instant messaging, and 2) data sent to websites and identity when communicating with a website.

In most email and chat services, the messages are not encrypted but transferred as plain text. Data can be protected, however, through the use of cryptographic methods that convert it from readable plain text into ciphertext. Most email encryption standards, such as Pretty Good Privacy (PGP), use a combination of symmetric key and public key cryptography.

One way of encrypting messages is to add encryption manually with additional software or a plug-in that implements the PGP standard. The Enigmail PGP add-on for Mozilla Thunderbird or the Mailvelope browser plug-in can be used for this purpose. However, due to the relatively high barrier to entry in terms of technical knowledge and the continuous task of key exchange, email encryption is not widely used.

As an alternative to software and plug-ins that require configuration and maintenance from users, more and more email services provide encrypted messaging. For example, both Tutanota and ProtonMail are free and open-source email services that offer encrypted messaging within the service. Both are zero-knowledge systems, that is, they encrypt message content and user data on the client side before transferring them to their servers. The user's password serves as the key for decrypting the content. As the password is not stored by the email service, the service cannot access the content of the messages. Meanwhile most email services, such as Gmail, send data to their servers unencrypted.

Groups and individuals at risk of surveillance, such as NGOs, are encouraged to use encrypted

messaging. Whistle-blowers also need to be capable of using this technology, paired with anonymizing tools that enable them to mask their identities.

Users also reveal personal information when they visit. Here again, they should use precaution when sending unencrypted content such as form data. They also reveal an additional piece of information when they visit a website: their location. When a user opens a website, the IP address is communicated to the site. The IP address can reveal the identity of the user by enabling network communication to be traced back to them. There are ways of hiding the IP address though, for instance, by using a Virtual Private Network (VPN) server or by routing the traffic through a network as does The Onion Router (Tor), described below.

But not only the IP address incorporates potentially sensitive information. Even if the content of messages is encrypted, patterns of communication such as who is communicating with whom, how often, how rapidly and how frequently can reveal information about the participants and their relationship. This information is contained in the unencrypted part of the message: the header, which includes the source, destination and time of the communication. The inspection of these data is called traffic analysis.[48]

One way of circumventing surveillance by traffic analysis is by using a VPN service. VPN servers work as a proxy: the user's request is first sent to the VPN server before being transferred to the target site. In the same way, the target site's response is first sent to the VPN server then transferred to the user. This way the target site will only learn the IP address of the VPN server, not the one from which the request was initiated. As an example for a free VPN service, Opera browser now offers a built-in VPN server.[49]

Another option is to use onion routing. Onion routing-based communication anonymizing tools allow users to anonymously browse the web. Onion routing works by distributing communication over several places on the Internet. The higher the number of participants, the more security is increased as transactions become less and less traceable.

---

[48] *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en.
[49] A thorough overview of the options for different use vases can be found at *How to Choose the Best VPN Service for Your Needs*, HOW-TO GEEK, http://www.howtogeek.com/221929/how-to-choose-the-best-vpn-service-for-your-needs.

The largest system to have implemented onion-routing technology is Tor, which drew more than four million daily users as of early November 2015.[50] The mechanism of achieving encryption and anonymity within Tor is as follows:

> [D]ata packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.
>
> To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.[51]

Besides being an effective tool for masking the origin and destination of communication, Tor can also be used as a censorship circumvention tool, allowing its users to reach sites that are blocked by the Internet service provider in their location due to Internet censorship. The Tor documentation also notes that Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features. In addition, Tor features hidden services that let users publish web sites or operate chat servers without having to reveal the location of the host.

However, while providing anonymity in the face of network analysis, there are other identification methods that remain effective even if a user is using Tor, such as setting tracking cookies or identification via browser fingerprint. We will review these threats in the following section.

Whistle-blowers can use Tor to communicate more safely with journalists. NGOs can benefit from Tor to allow their workers to connect to their home website while they are in a foreign country, without notifying everybody nearby that they are working with that organization.

---

[50] *Estimated number of clients on the Tor network*, TOR METRICS, https://metrics.torproject.org/clients-data.html.
[51] *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en.

C. Browsing

Browsing may reveal even more in-depth information if users' browsing habits are followed across websites, and a tracker records which sites users visited and how frequently. Trackers collect information not only about which websites users are visiting, but information about their devices as well. Tracking users' browsing habits is a rich source of information that enables trackers such as data brokers or advertising companies to build a comprehensive profile of a person: their age, where they live, what they read, what they are interested in, their health issues and life management concerns, their sexual orientation and more. This information can then be packaged and sold to others: advertisers, other companies, or governments.

Many websites host a variety of trackers. A subset of trackers is present for the purpose of analytics, that is, to collect information about the website for the owner. Many others, however, are there to transfer users' browsing information to companies who collect and sell data. This data is highly valuable to advertisers who use it to target ads specifically to customers based on their behaviors.

Many companies that track users are not related to the visited site. They are advertisers or analytics companies, such as DoubleClick (owned by Google) or ComScore. They pair up with data broker companies who aim to compile a comprehensive profile of users and ultimately aim to link the information to their offline identities.[52]

Facebook, Google and Twitter also track user behavior on many sites simply by the "Like' or G+ or tweet icons.

Another form of tracking is done through the use of HTTP cookies. An HTTP cookie is a small data file that is set by a website and stored in a user's web browser while the user is browsing that website. When the user loads the website, the browser sends the cookie back to the server (unless the user deletes the cookie). The next time the user visits that website, the server can find the data that has already been stored about the user's previous visits and settings.[53]

---

[52] Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you.
[53] Adam Barth, "Overview," *HTTP State Management Mechanism*, INTERNET ENGINEERING TASK FORCE (April 2011), https://tools.ietf.org/html/rfc6265#section-3.

Initially cookies were designed to enable websites to remember information such as items in a shopping cart, user preferences or to record the user's browsing activity such as time of previous logins or history of visited pages. Some cookies are set by the website the user is visiting. This is called a first-party cookie. Third-party cookies, however, belong to domains other than the one the user visits. Third-party cookies can be activated when a web page loads content from other websites, such as advertisements or share icons. When a user 'accepts cookies,' the user not only allows first party cookies that serve the chosen website but also all of the trackers present on the site. This opens up the potential for tracking the user's browsing history as third-party trackers forward information to advertising and data broker companies.

As analyzed by webcookies.org as of 2015 November, some websites were setting cookies that were readable by over 100 third-party domains.[54] The average number of cookies set by one website was sixteen, with a maximum of 463 (which includes first and third party cookies).[55]

Even for users who browse using anonymization tools such as Tor, cookies can be revealing. For instance, if the user visits a site to which a national security agency has access, the website creates a cookie on the user's browser and stores a real IP address and other personal information about the user. When the same user visits the same website again, and enables Tor this time on the same browser, then the website will read the last stored cookie, which includes the user's real IP address and other personal Information. This way it is possible to link the activity back to the user's real IP address.[56]

However, HTTP cookies are not the only technology pertinent to the web tracking context: there are different technologies that can be used to link one user's web browsing activities together.

Supercookies are like standard HTTP cookies, but they are stored in different locations on a user's machine, for example, in a file used by a plug-in like Flash. As a result they are harder to find and delete. As the browser searches at set locations when it tries to detect the cookies, it does not find and remove them either. Furthermore, some supercookies have additional capabilities, like regenerating regular cookies to prevent their removal by the user.[57]

---

[54] *Third party domains*, WEB COOKIES SCANNER, http://webcookies.org/third-party-cookies.
[55] *Cookie number statistics*, WEB COOKIES SCANNER, http://webcookies.org/number-of-cookies.
[56] Mohit Kumar, *NSA using Browser Cookies to track Tor Users*, THE HACKER NEWS (Oct. 5, 2013), https://thehackernews.com/2013/10/nsa-using-browser-cookies-to-track-tor.html.
[57] Julia Angwin, *Latest in Web Tracking: Stealthy 'Supercookies'*, WALL STREET J. (Aug. 18, 2011),

As a result of their web survey, engineering researchers McDonald and Cranor report extensive use of Flash cookies capable of uniquely identifying computers or recreating deleted cookies.[58] Zombie cookies are cookies that are automatically recreated after being deleted. This is accomplished with the help of a client-side script.

Another tracking technology is a web beacon. A web beacon is an object embedded in a web page or email, which invisibly allows it to check that a user has accessed the content of the web page or email via an invisible, 1x1 pixel image placed on the site or using an HTML tag. For example, this way companies can track the effectiveness of their e-mail content or identify their most active users.

Tracking can also be achieved even without relying on such external technologies. Taking its settings together, a browser's specific configuration can be sufficiently unique that it can be distinguished from others which also enables tracking. On the Panopticlick website of the Electronic Frontier Foundation one can measure how unique their browser configuration is.[59] Peter Eckersley conducted research on nearly 500,000 browsers in 2010 and found that 83.6% could be uniquely identified by fingerprinting.[60] Ninety-four point two percent of browsers enabled with Flash or Java were uniquely identified.[61] It is especially hard to mask this information as attempts at masking may make the browser configuration even more unique.

Several tools exist to block a third-party from loading content on a webpage. Privacy Badger automatically blocks an advertiser from loading any more content into the user's browser if the advertiser seems to be tracking the user across multiple websites without their permission. Ghostery, on the other hand, blocks content based on a categorized tracker list.

D. Data Storage

Storing personal and work-related documents in the cloud via cloud service providers has

---

http://www.wsj.com/articles/SB10001424053111903480904576508382675931492.
[58] Aleecia M. McDonald & Lorrie Faith Cranor, *A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies*, CYLAB (Jan. 31, 2011), https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11001.pdf.
[59] PANOPTICLICK, https://panopticlick.eff.org.
[60] Peter Eckersley, How unique is your web browser?, *in* PRIVACY ENHANCING TECHNOLOGIES 1, 1 (Mikhail Atallah & Nicholas Hopper eds., 2010).
[61] *Id*.

become ubiquitous. In this case, users need to protect their documents from access by or through the service provider. Users should apply similar precautions in order to keep the files on their own computers safe from external access. Encryption technologies can be used to protect data stored in the cloud or on the hard drive.

In the case of cloud-based storage, to achieve end-to-end encryption from the user's computer to the server, data may be encrypted manually by the user and uploaded to the service provider.

A few end-to-end encrypted, zero-knowledge solutions also exist, such as SpiderOak and Mega. These providers ensure that only the user has access to the stored documents in unencrypted form; not even providers themselves have access.

For offline storage, BitLocker, DiskCryptor, FileVault or VeraCrypt are examples of software that provide encryption for whole volumes or individual folders.[62]

CONCLUSION

Privacy and data protection are fundamental rights that governments and business groups should not violate. First of all, it is the government's task and responsibility to set up a legal environment protecting these rights. Further, the obligation to respect the right to private life and the protection of personal information is a binding obligation both on the public and the private sector. The authors strongly believe that citizens should not feel obligated to adjust their behavior in order to keep their privacy and data protected.

Nevertheless, the Snowden revelations and other experiences have proved that laws do not provide adequate safeguards and that neither governments nor businesses reliably refrain from violating citizens' and users' privacy and protected data. Therefore, while as a traditional human rights NGO the HCLU is still fighting for adequate laws and implementation thereto, we also recognize the need to educate people and offer specific empowerment tools through technology. Our internal solution to this dilemma is that as long as laws do not provide adequate safeguards, everyone can and should protect

[62] As a potential future solution, homomorphic encryption1 is a promising research area with applications in cloud-based data storage: it allows computation on encrypted data without decrypting, that is, without looking into it. The technique would make it possible to store, analyze, and get back results from personal data online, all in encrypted form.

their online privacy.

Through the Right to Hide website, we offer simple, hands-on tools to make effective enjoyment of privacy available for more people. This shift in focus brings its own challenges. In order to widen the reach of the project, we plan to organize training sessions for the specific target groups. Thus the organization needs not only technological but also training capacity. We need to teach technical skills while also raising awareness about the possible threats to privacy and help Internet users overcome the mental barriers that thwart their entry into the technological sphere.

We launched the Right to Hide website in mid-January, 2016. We have already conducted one training session as part of a hackathon for NGOs, and are planning to organize others. Here again, though, we see the importance of expanding our mission beyond NGOs alone. Thus, we hope to offer two main training tracks including workshops for NGOs and journalists as well as training in schools to raise awareness about privacy issues. These sessions are all part of the project's larger mission to empower Internet users with tools, skills, and a new mindset because online privacy cannot be protected offline.