

Estonia

	2013	2014		
Internet Freedom Status	Free	Free	Population:	1.3 million
Obstacles to Access (0-25)	1	1	Internet Penetration 2013:	80 percent
Limits on Content (0-35)	3	3	Social Media/ICT Apps Blocked:	No
Violations of User Rights (0-40)	5	4	Political/Social Content Blocked:	No
TOTAL* (0-100)	9	8	Bloggers/ICT Users Arrested:	No
			Press Freedom 2014 Status:	Free

* 0=most free, 100=least free

Key Developments: May 2013 – May 2014

- Estonia continues to be one of the most wired countries in the world, with increasing internet access and online participation among citizens (see **Obstacles to Access**).
- In October 2013, the European Court of Human Rights upheld an Estonian Supreme Court decision from 2009 stating that content hosts may be held legally liable for third-party comments made on their website (see **Limits on Content**).
- Estonia continues to improve its cybersecurity programs, strengthening its capacity to prevent and combat cyberattacks (see **Violations of User Rights**).

Introduction

Estonia ranks among the most wired and technologically advanced countries in the world. With a high internet penetration rate, widespread e-commerce, and e-government services embedded into the daily lives of individuals and organizations, Estonia has become a model for free internet access as a development engine for society. When the country regained independence in 1991 after nearly 50 years of Soviet rule, its infrastructure was in a disastrous condition. The country's new leadership, however, perceived the expansion of information and communication technologies (ICTs) as a key to sustained economic growth and invested heavily in their development.

The first internet connections in the country were introduced in 1992 at academic facilities in Tallinn and Tartu. The national telecommunication monopoly was subsequently privatized with the inclusion of Finnish and Swedish telecommunication companies, and a fiber-optic backbone was built with modern fixed and mobile communications services. The government further worked with private and academic entities to initiate a program in 1996 called Tiger Leap, which aimed to establish computers and internet connections in all Estonian schools by 2000. This program helped to build a general level of technological competence and awareness of ICTs among Estonians. Today, with a high level of computer literacy and connectivity already established, the program's focus has shifted from basic concerns such as access, quality, and cost of internet services to discussions about security, anonymity, the protection of private information, and citizens' rights on the internet. Children's safety on the internet is a high priority, and the special program "Targalt Internetis" (Wiser Internet) is dedicated to country-wide training and awareness-building activities on internet safety issues for parents and children. In addition, a majority of users conduct business and e-government transactions over the internet: in 2013, nearly 97 percent of banking transactions were done with e-banking services and 95 percent of people declared their income electronically.¹

On October 10, 2013, the European Court of Human Rights issued a ruling that reaffirmed an earlier Estonian Supreme Court decision regarding the legal liability of content hosts for third-party comments. The ECtHR found that a company's legal liability for comments posted by its users did not sufficiently interfere with the freedom of expression guarantees enshrined in the European Convention on Human Rights; therefore, intermediaries could be held responsible for third-party content published on their website or forum, even if they delete the content upon notification.²

Additionally, over the past year, the issue of privacy for individual users on the internet became a widely debated topic in Estonia, with a particular focus on the privacy policies of global service providers. The Digital Agenda 2020 for Estonia, established by the Ministry of Economic Affairs and Communications, outlines how both technological and organizational conditions will be developed to ensure that people would always know and be able to decide when, by whom, and for what purpose their personal data is being used in the public sector.³

1 Estonian Information System's Authority, "Facts about e-Estonia," accessed June 1, 2014, <https://www.ria.ee/facts-about-e-estonia/>.

2 Case of Delfi AS v. Estonia, Judgement, accessed April 12, 2014, [http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{"itemid":\["001-126635"\]}](http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{).

3 Digital agenda 2020 for Estonia, accessed June 14, 2014, <http://www.riso.ee/en/information-society>.

Obstacles to Access

The number of internet and mobile telephone users in Estonia has grown rapidly in the past 20 years. According to statistics from the International Telecommunication Union (ITU), internet penetration in Estonia reached 80 percent in 2013, compared to about 78 percent in 2012 and 71 percent in 2008.⁴ There were also over 2 million mobile phone subscriptions, translating to a mobile phone penetration rate of 160 percent.⁵ This figure is commonly attributed to the widespread use of mobile internet access devices, the growing popularity of machine-to-machine (M2M) services, and the use of more than one mobile phone by individual Estonians.

The first public Wi-Fi area was launched in 2001, and since then the country has developed a system of mobile data networks that enable widespread wireless broadband access. In 2011, the country had over 2,440 free, certified Wi-Fi areas meant for public use, including at cafes, hotels, hospitals, schools, and gas stations, and the government has continued to invest in public Wi-Fi.⁶ In addition, a countrywide wireless internet service based on CDMA technology has been deployed and is priced to compete with fixed broadband access. Three mobile operators cover the country with mobile 3G and 3.5G services, and as of May 2013, 4G services covered over 95 percent of Estonian territory. Municipalities in rural areas have been subsidizing local wireless internet deployment efforts, and the country's regulatory framework presents low barriers to market entry, enabling local startups to proliferate.

Estonians use a large variety of internet applications, including search engines (85 percent of users), email (83 percent of users), local online media, news portals, social-networking sites, instant messaging, and Voice over Internet Protocol (VoIP) services.⁷ Estonian Public Broadcasting delivers all radio channels and its own TV production services, including news in real time over the internet; it also offers archives of its radio and television programs at no charge to users.

The Estonian Electronic Communications Act was passed in late 2004, and a number of amendments have been added to help develop and promote a free market and fair competition in electronic communications services.⁸ Today, there are over 200 operators offering such services, including six mobile phone companies and numerous internet service providers (ISPs). ISPs and other communications companies are required to register with the Estonian Technical Surveillance Authority (ETSA), a branch of the Ministry of Economic Affairs and Communications, though there is no registration fee.⁹

In 2009, the Estonian Internet Foundation was established to manage Estonia's top level domain,

4 International Telecommunication Union (ITU), "Percentage of individuals using the Internet, fixed (wired) Internet subscriptions, fixed (wired)-broadband subscriptions," 2013, accessed July 1, 2014, <http://www.itu.int/net4/itu-d/icteye/>.

5 International Telecommunication Union (ITU), "Mobile-cellular subscriptions," 2013, accessed July 11, 2014, <http://www.itu.int/net4/itu-d/icteye/>.

6 Public Wi-Fi Hotspot database in Estonia, accessed July 30, 2013, <http://kaardistajad.wifi.ee/avalik.php>.

7 Pille Pruulmann-Vengerfeldt, Margit Keller, and Kristina Reinsalu, "1.1.4 Quality of Life and Civic Involvement in Information Society," *Information Society Yearbook 2009* (Tallinn: Ministry of Economic Affairs and Communications, 2010), <http://www.riso.ee/en/pub/2009it/#p=1-1-4>.

8 "Electronic Communications Act," Ministry of Economic Affairs and Communications, accessed March 26, 2009, <http://www.mkm.ee/index.php?id=9576>.

9 Estonian Technical Surveillance Authority (ETSA), "Commencement of Provision of Communications Service," accessed February 15, 2014, <http://www.tja.ee/index.php?id=11703>.

“.ee.”¹⁰ With its multi-stakeholder foundation, the organization represents the Estonian internet community internationally and has succeeded in overseeing various internet governance issues such as the domain name registration process. After initial concerns over the foundation’s domain registration pricing policy¹¹ and management capabilities,¹² the foundation’s substantive work was stabilized in 2012-2013. In February 2012, the Estonian Internet Foundation was admitted to the Council of European National Top Level Domain Registries (CENTR).

Limits on Content

Restrictions on internet content and communications in Estonia are among the lightest in the world. YouTube, Facebook, Twitter, LinkedIn and many other international video-sharing and social-networking sites are widely available and popular. Moreover, 32 percent of Estonians use the internet for uploading and sharing original content such as photographs, music, and text—the highest level of shared public communication in Europe.¹³ Nevertheless, due in part to Estonia’s strong privacy laws, there are some instances of content removal. Most of these cases involve civil court orders to remove inappropriate or off-topic reader comments from online news sites. Comments are similarly removed from online discussion forums and other sites. Generally, users are informed about a given website’s privacy policy and rules for commenting, which they are expected to follow. Most of the popular online services have established policies that outline a code of conduct for the responsible and ethical use of their services and have enforcement policies in place.

In 2008, a debate over self-censorship and pre-publication censorship took center stage when the victim of unflattering and largely anonymous comments on a news story filed suit against the popular Estonian news site *Delfi*, claiming that the web portal must be held responsible for defamatory reader comments and screen them before they become public.¹⁴ In 2009, the Estonian Supreme Court upheld the rulings of the lower courts, stating that *Delfi* is not a passive intermediary since the site already exerts control over the comments section by removing those that violate their own rules; therefore, it can be held liable for defamatory or otherwise illegal content prior to publication. Website owners argued that they did not have the capacity to monitor and edit all comments made on their sites. In October 2013, the European Court of Human Rights issued the final ruling on the case, upholding the Estonian Supreme Court ruling by stating that the company’s liability for defamatory comments was not a “disproportionate interference” with Article 10 of the European Convention on Human Rights, which guarantees freedom of expression.¹⁵

In another case regarding intermediary liability, the European Court of Justice issued a ruling on May 13, 2014, stating that the 1995 Data Protection Directive applied to the activities of search engines

10 Estonian Internet Foundation, accessed July 30, 2013, <http://www.internet.ee/en/>.

11 The activities of the Estonian Internet Foundation are not subsidized from the state budget; the registration fee covers infrastructure investments, operating costs, and reserve funds.

12 “Marek-Andres Kauts resigns as board member,” Eesti Internet, May 23, 2012, <http://www.internet.ee/news/?year=2012&month=5>.

13 “Individuals Using the Internet for Uploading Self-Created Content to Any Website to Be Shared,” Eurostat, accessed June 11, 2013, <http://appsso.eurostat.ec.europa.eu>.

14 Kaja Koovit, “Big Businessman Goes to War Against Web Portals,” Baltic Business News, March 18, 2008, <http://www.balticbusinessnews.com/?PublicationId=48694078-50cc-4fe1-b3e4-6e10bc6a5ec1>.

15 “European Court strikes serious blow to free speech,” ARTICLE 19, October 14, 2013, <http://www.article19.org/resources.php/resource/37287/en/european-court-strikes-serious-blow-to-free-speech-online>.

like Google, and that these companies may have to remove search results if the data is deemed to violate an individual's right to privacy. Cases in which search engines may have to remove links are limited only to searches for an individual's name; the original content in the link would not be removed and would still appear in other searches, but the link would no longer appear in search results for the individual who requested the removal. Many critics of this ruling argue that the court should not have granted private companies the authority to arbitrate competing concerns between the right to privacy and the right to information, and that the court failed to establish clear guidelines regarding when links to data should be removed.

In January 2010, a new law on online gambling came into force, requiring all domestic and foreign gambling sites to obtain a special license or face access restrictions. As of February 2014, the Estonian Tax and Customs Board had over 1,000 websites on its list of illegal online gambling sites that Estonian ISPs are required to block.¹⁶ The list of blocked sites is transparent and is available to the public.

Over the past few years, the removal of online content related to possible copyright infringement on YouTube and other video streaming services has increased, resulting in the removal of over 80,000 videos. This process was greatly facilitated by requests from copyright enforcement organizations representing Estonian authors.¹⁷ Hundreds of videos have been removed from YouTube for copyright violations even though some of the videos were posted by the authors themselves who were apparently not aware of the activities of copyright enforcement organizations representing their rights.¹⁸ All of these requests came from individuals or companies; the Estonian government has not issued any requests for removal of content on any of Google's platforms, including YouTube, since at least 2010.¹⁹

There are over 70,000 active Estonian-language blogs on the internet, including an increasing number of group, project, and corporate blogs. The vibrancy and activities of the blogosphere are frequently covered by traditional media, particularly when blog discussions center on civic issues. The fact that so many Estonians are both computer literate and connected to the internet has created unique opportunities for the Estonian government. In addition to hosting virtual trade fairs and an online embassy, the Estonian president's office has its own Twitter and Facebook accounts, and releases messages on its YouTube channel.²⁰

Estonia has the largest functioning public-key infrastructure²¹ in Europe, based on the use of

16 The list of restricted websites can be found on the Estonian Tax and Customs Board website: "Ebaseadusliku kaughasartmängu serverite domeeninimed" [Illegal gaming servers, domain names], Tax and Customs Board, accessed June 10, 2014, http://www.emta.ee/public/Kontroll/MTA_must_nimekiri_25.02.2014.pdf.

17 "Preliminary report," Project 451, Institute of Digital Rights, accessed June 17, 2013, <http://451.ee/en/preliminary-report/>.

18 "Autorite ühing laseb YouTube'ist videoed eemaldada," ERR News, February 2, 2011, <http://uudised.err.ee/index.php?06223519>.

19 Google Transparency Report, "Estonia – Removal Requests," accessed July 11, 2013, <http://www.google.com/transparencyreport/removals/government/EE/>

20 "Estonia Launches Embassy in Virtual World Second Life," Sydney Morning Herald, December 5, 2007, <http://www.smh.com.au/news/Technology/Estonia-launches-embassy-in-virtual-world-Second-Life/2007/12/05/1196530704693.html>; "Estonian President Launches YouTube Video Blog," TopNews.in, December 9, 2008, <http://www.topnews.in/estonian-president-launches-youtube-video-blog-297028>.

21 A public-key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates, which are used to verify that a particular public key belongs to a certain entity. The PKI creates digital certificates that map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed.

electronic certificates maintained on the national identification (ID) card.²² More than 1.2 million active ID cards are in use, which enable both electronic authentication and digital signing, and over 40 percent of active ID cards have been used for authentication and digital signature purposes.²³ The Digital Signature Act, adopted in 2000,²⁴ gives an individual's digital signature the same weight as a handwritten one and requires public authorities to accept digitally-signed documents. Estonian ID cards were used to facilitate electronic voting during the parliamentary elections in 2007 and were used again in the 2009 municipal and European Parliament elections. During the 2014 European Parliament elections, 103,151 votes were cast over the internet, representing over 31 percent of all votes from Estonia.²⁵ In 2013, 95 percent of citizens filed their taxes online, making the web services offered by the tax department the most popular public e-service. Over 63 percent of internet users regularly use e-government services, and 77 percent of these users have indicated their satisfaction with such services.²⁶

Violations of User Rights

Freedom of speech and freedom of expression are protected by Estonia's constitution and by the country's obligations as a member state of the European Union. Anonymity is unrestricted, and there have been extensive public discussions on anonymity and the respectful use of the internet. Internet access at public access points can be obtained without prior registration. Over the past few years, the government has succeeded in reducing the number and severity of cyberattacks against its infrastructure.

The Personal Data Protection Act (PDPA), first passed in 1996, restricts the collection and public dissemination of an individual's personal data. No personal information that is considered sensitive—such as political opinions, religious or philosophical beliefs, ethnic or racial origin, sexual behavior, health, or criminal convictions—can be processed without the consent of the individual. The Data Protection Inspectorate (DPI) is the supervisory authority for the PDPA, tasked with “state supervision of the processing of personal data, management of databases and access to public information.”²⁷ The current version of the PDPA came into force in 2008.²⁸

Estonia is currently in the process of amending the Penal Code to comply with the European Council Framework Decision 2008/913/JHA²⁹ of 28 November 2008 on “combating certain forms and expressions of racism and xenophobia by means of criminal law” in order to establish a framework

22 See the web portal for the ID-card system, <http://id.ee/?lang=en>.

23 Ibid., accessed July 15, 2013.

24 “Digitaalalkirja seadus” [Digital Signature Act], Riigi Teataja, accessed May 21, 2013, <https://www.riigiteataja.ee/akt/694375>.

25 “Statistics about Internet Voting in Estonia,” Vabariigi Valimiskomisjon (Electoral Commission), accessed August 2014, <http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics>.

26 Kristina Randver, *Kodanike rahulolu riigi poolt pakutavate avalike e-teenustega, Jaanuar 2010* [Citizens' Satisfaction with the Provision of Public E-Services, January 2010] (Tallinn: TNS Emor, 2010), http://www.riso.ee/et/files/kodanike_rahulolu_avalike_eteenustega_2010.pdf.

27 Electronic Privacy Information Center (EPIC) and Privacy International, “Republic of Estonia,” in *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (Washington: EPIC, 2007), <http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-8.html>.

28 Estonian Data Protection Inspectorate, “Inspectorate,” March 14, 2013, <http://www.aki.ee/en/inspectorate>.

29 EUR-Lex, “Access to European Union Law,” accessed May 5, 2013, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0913:en:NOT>.

on hate speech criminalization in the country. In July 2012, the Ministry of Justice initiated proceedings to amend sections 151 and 152 of the penal code, which would lead to a new legal norm regarding hate speech-related legislation in Estonia.³⁰ This process is still ongoing and has become the topic of significant public debate within the country.

Estonia launched the Electronic Communications Act on January 1, 2005, aligning itself with EU legislation and replacing the Telecommunications Act. Since January 2008, electronic communications companies have been required to preserve traffic and location data for one year, as defined by the EU Data Retention Directive (2006/24/EC). Companies have been required to retain data on internet access, telephony, and email since March 2009, and must only retain such data that becomes known to them in the course of providing communications services. They must also provide the surveillance agency or security authority with the information at their disposal only when presented with a court order.³¹

However, data retention practices in Estonia and other European Union member states were recently thrown into doubt by the European Court of Justice (ECJ).³² On April 8, 2014, the court found the European Data Retention Directive (2006/24/EC) to be invalid and in contravention of articles 7, 8, and 52(1) of the European Convention on Human Rights. The ruling was lauded among privacy proponents who had long argued that requirements for the blanket retention of data constituted mass surveillance and far exceeded what was necessary for law enforcement purposes. However, the decision has also prompted debate among legal experts, with some member states now suspending their national implementations of the European directive, while others are drafting new data retention laws in order to compel internet service providers to continue to store user data.³³

According to the report of the Estonian Parliament Security Authorities Surveillance Select Committee that oversees the practices of surveillance agencies and security agencies, there were over 7,400 cases of requests for information based on court orders in 2012, an increase of 9 percent from the previous year.³⁴ The select committee has been established to exercise supervision over the legality of surveillance and the activities of the Security Police.³⁵ The committee monitors the conformity of the activities of the Security Police Board with the constitution, the Surveillance Act, and other regulations on security agencies.

There have been no physical attacks against bloggers or online journalists in Estonia, though online discussions are sometimes inflammatory. Following instances of online bullying, sexual harassment,

30 Office of the High Commissioner for Human Rights, "Tenth and Eleventh Periodic Report on the implementation of the International Convention on the Elimination of all forms of Racial Discrimination in Estonia," January 2013, <http://www2.ohchr.org/English/bodies/cerd/docs/CERD.C.EST.10-11.docx>.

31 Electronic Communications Act, translation to English, <http://www.legaltext.ee/text/en/X90001K2.htm>.

32 The ECJ court ruling pertained to the cases *Digital Rights Ireland Ltd* (C-293/12) and *Kärntner Landesregierung* (C-594/12) and is available at <http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN>.

33 Martin Husovec, "First European Constitutional Court Suspends Data Retention After the Decision of the Court of Justice of EU," The Center for Internet and Society at Stanford Law School, April 28, 2014, <http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court>.

34 Overview of Parliament Select Committee activities, http://www.riigikogu.ee/public/Riigikogu/Dokumendid/julgeolekuasutuste_jarelevalve_erikomisjon_2012.pdf.

35 "Security Authorities Surveillance Select Committee," Riigikogu: The Parliament of Estonia, April 4, 2011, http://www.riigikogu.ee/index.php?id=42701&parent_id=34615.

and the misuse of social media in 2009-2010, discussions and public awareness campaigns were launched to involve parents in increasing the protection of children on the internet.³⁶

Awareness of the importance of ICT security in both private and business use has increased significantly since the cyberattacks that occurred in the spring of 2007. To protect the country from future attacks, the government adopted a five-year Cyber Security Strategy in 2008 that focused on the development and implementation of new security measures, increasing competence in cyber security, improving the legal framework, bolstering international cooperation, and raising public awareness.³⁷ Estonia's cybersecurity strategy is built on strong private-public collaboration³⁸ and a unique voluntary structure through the National Cyber Defense League.³⁹ With more than 150 experts participating, the league has simulated different security threat scenarios over the past few years as defense exercises that have served to improve the technical resilience of Estonia's telecommunication networks and other critical infrastructure.

Also in 2008, the North Atlantic Treaty Organization (NATO) established a joint cyberdefense center in Estonia to improve cyberdefense interoperability and provide security support for all NATO members. Since its founding, the center has supported awareness campaigns and academic research on the topic and hosted several high-profile conferences, among other activities.⁴⁰ From 2009, the NATO Cooperative Cyber Defense Centre of Excellence has organized an annual International Conference on Cyber Conflict, or CyCon, bringing together international experts from governments, the private sector, and academia. CyCon has focused on international cooperation and the legal, regulatory, military, and paramilitary aspects of cybersecurity, with the goal of ensuring the development of a free and secure internet.

36 Targalt internetis [awareness portal], accessed June 12, 2013, <http://www.targaltinternetis.ee>.

37 Cyber Security Strategy Committee, *Cyber Security Strategy* (Tallinn: Ministry of Defence, 2008), http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf.

38 Ibid.

39 "Estonian Defence League's Cyber Unit," Kaitseliit [Defence League], <http://www.kaitseliit.ee/en/cyber-unit>.

40 "Conference on Cyber Conflict," Cooperative Cyber Defense Centre of Excellence (CCD COE), accessed July 15, 2013, <http://www.ccdcoe.org/conference2010/>.