INTERNATIONAL MODERN MEDIA INSTITUTE

IMMI Research Report

Islands of Resilience

Comparative Model for Energy, Connectivity and Jurisdiction

Realizing European ICT possibilities through a case study of Iceland

Prepared at the request of:

The Greens | European Free Alliance in the European Parliament

on behalf of Members of the European Parliament
Christian Engström, Indrek Tarand, Carl Schlyter, Sandrine Bélier, Karima Delli, Eva Lichtenberger, Raül Romeva i Rueda, Heide Rühle, Judith Sargentini, Bas Eickhout and Marije Cornelissen

Smári McCarthy

Eleanor Saitta

Islands of Resilience:

Comparative Model for Energy, Connectivity and Jurisdiction

Realizing European ICT possibilities through a case study of Iceland

Smári McCarthy · Eleanor Saitta

International Modern Media Institute

2012

Prepared at the request of:

The Greens | European Free Alliance
in the European Parliament

on behalf of Members of the European Parliament
Christian Engström, Indrek Tarand, Carl Schlyter, Sandrine Bélier, Karima Delli, Eva Lichtenberger, Raül Romeva i Rueda, Heide Rühle, Judith Sargentini, Bas Eickhout and Marije Cornelissen

Produced at the request of
Members of the European Parliament:

Christian Engström
Indrek Tarand
Carl Schlyter
Sandrine Bélier
Karmima Delli
Eva Lichtenberger
Paül Romeva i Rueda
Heide Rühle
Judith Sargentini
Bas Eickhout
Marije Cornelissen

Authors:
Smári McCarthy
Eleanor Saitta

Layout:
Jonas Smedegaard
Smári McCarthy

Contributing Researchers:
Guðjón Idir
Jason Scott

Online Support:
Jonatan Walck
Jonas Smedegaard

Photo credits:

Smári McCarthy	(cover, road, waterfall, island; CC-BY)
James Cridland	(Alþingi; CC-BY)
Stuck in Customs	(geyser; CC-BY-NC-SA)

IMMI – International Modern Media Institute

The viewpoints in this report belong to the authors, and they may not necessarily concur partially or wholly with IMMI's viewpoints as an institute.

Table of Contents

Abstract....4
Introduction....5
Model and Methodology....6
Modelling Iceland....7
Energy....9
Energy Model....10
Analysis of Iceland....11
Connectivity....19
Connectivity Model....20
Analysis of Iceland....21
Jurisdiction....29
Jurisdiction Model....30
Analysis of Iceland....31
Icelandic Modern Media Initiative....41
Freedom of Information Act....43
Network Neutrality....44
Communications Protection and Communications Data Retention....45
Intermediary Liability Limitations....46
Libel Tourism Protection....47
Libel Reform and Publishing Liability Limitations....48
Whistleblower Protection....49
Prior Restraint Limitations....50
Virtual Limited Liability Companies....51
Selected Bibliography....53
Appendix A: Model Details....54
Energy....54
Connectivity....57
Jurisdiction....62

Abstract

Locale is rapidly becoming one of the most important competitive differentiators in the provision of cloud-based information technology services. Broadly speaking, three categories of issues define a locale's fitness for hosting the cloud: energy, connectivity, and jurisdiction.

Energy is the largest cost center for most cloud hosts. Beyond price per kilowatt hour, hosting companies must consider redundant network availability, power grid resilience, environmental sustainability, climate, and equipment cooling requirements as core parts of their energy strategy.

Connectivity is clearly essential for hosts, and differentiating factors here include total installed bandwidth, current utilized bandwidth, hub redundancy, international uplink redundancy, round trip latency, traffic shaping and network neutrality.

Jurisdictional issues are an area of emerging concern and awareness for cloud hosts, where the landscape is shifting rapidly. Hosting companies are deeply affected by intermediary liability, hosting liability, state and corporate surveillance, state and corporate censorship, the accessibility of and cost of interacting with courts, corruption, and socioeconomic stability.

This report considers Iceland's relative competitive advantages and drawbacks as a hosting locale relating to these issues.

Introduction

In January 2012, the authors of this paper wrote a preliminary study intended to give a birds-eye view of the primary factors pertaining to energy, connectivity and jurisdiction in Iceland, as applicable to ICT[1] growth in general and cloud hosting in particular. We were interested in exploring the possibilities available for Iceland in terms of ICT development, and found that there were clear advantages that Iceland had in relation to ICTs, although there were also some substantial weaknesses.

From the beginning, it was clear that a more thorough study would be required, in particular focused on the development of a generalized comparative model for energy, connectivity and jurisdiction, with the goal of making it possible to compare any two countries or regions.

With this model, which is based on almost 80 variables, we intend to lay the groundwork for further investigations into the European ICTs sector, while also giving insights into the Icelandic situation as previously analyzed, when seen through the lens of this model.

In particular, we focus on the question of resilience. While it is traditional to consider the sustainability and the economic viability of projects, in particular in the ICTs sector, it is rarer to see a holistic investigation from the standpoint of what can possibly fail. Analyzing the failure modes in a system is often more important than analyzing the operation modes: understanding how systems crash is the first step towards preventing them from doing so. As a result, throughout this study, we emphasize on redundancy, reliability, elasticity, expansionary capacity and reaction to systemic burden.

Our hope is that with this model, it will be possible to identify islands of resilience in a sea of insecurity.

Model and Methodology

Central to this paper is an analytical model which provides a method for comparing different countries, or regions within countries, on the basis of access to energy, connectivity and jurisdiction. Among the factors taken into account are energy source scalability, renewability and price, generation redundancy grid reliability, environmental factors such as cooling and insulation; redundancy, latency, throughput and other factors concerning connectivity both generally and with particular regions, and jurisdictional burdens stemming from surveillance, censorship, monopolies, software patents, frivolous libel action, value added tax, and access to human resources. While extensive in scope, the model is relatively easy to interact with and affords the discovery of key features and vulnerabilities a jurisdiction.

The categories represented in the model represent the understanding of the authors as to those factors that meaningfully distinguish one jurisdiction from another for the provision of cloud hosting services. We base this understanding both on our experience as technologists and conversations with others in the industry, and on the specific factors we have seen companies taking into account as they place new data centers, particularly as the cloud hosting market becomes increasingly competitive and commoditized. As no historical data exists for the cloud hosting market against which a rubric could be tested, we use a simple accumulative, flatly-weighted model. Organizations using the model as an analytic tool with specific jurisdictional requirements may find it useful to weight the model to better reflect their requirements.

Each of the following chapters will begin with an introduction to the model's questions and the rubrics by which the score is determined. Following this will be analysis of the situation in Iceland, in order to provide a practical template for how the model can be applied in practice.

The model asks a number of questions for which the answers will likely not be the same for all areas of a country. The analysis should focus on a specific region of the country which is both relevant for hosting and for which the answers generally hold true. Needless to say, the analysis must focus on the same region for all parts of the model.

Modelling Iceland

Iceland scored a total of 3.82 out of a total of 5 in our comparative model, gaining a total of 281 points. A complete breakdown of scores for each chapter are in the respective chapter. The full questions and rubrics for each metric are listed in Appendix A.

Chapter	Score
Energy	4.25
Connectivity	3.58
Jurisdiction	3.62

Category	Available points	Iceland points
Energy Sources	15	12
Energy Generation	10	9
Power Grid	10	8
Environmental Factors	25	17
Domestic Connectivity	45	33
Connectivity to Central/Western Europe	30	27
Connectivity to North America	30	23
Connectivity to Eastern Europe/Russia	30	21
Connectivity to Middle East and North Africa	30	16
Connectivity to East/Southeast Asia	30	16
State Security Burdens	25	21
Competitive Landscape	35	30
Commercial Issues	30	10
Legal Friction	20	18
Human Resources	25	19

Iceland's key strengths are:

1. Cheap and abundant energy generated from green, renewable, sustainable and resilient energy sources, distributed over a well designed and resilient power grid.
2. Increasingly good connectivity to the outside world with reasonable redundancy and a large amount of unused capacity available for expansion, and a very highly developed internal network with high resiliency.
3. An advanced and stable jurisdiction, with clear information rights and regulations, well structured administration, and well informed governing bodies.

Iceland's main weaknesses are:

1. Scale discrepancies both in energy generation and consumption which could potentially threaten grid resilience in extreme cases. This can be improved with further diversification of energy consumers, such as large-scale ICT deployments.
2. Iceland's data connectivity is provided by a relatively small number of submarine cables connecting to the outside world, creating some network precarity. This is currently being improved with the addition of new cables.
3. International data transport bandwidth through submarine cables is currently expensive. This could be mitigated by further investments, subsidies, or other methods to reduce the price for connection, with the intention of increasing the overall usage.
4. Iceland has similar issues with blanket communications surveillance as in the EU, which make it less attractive for hosting than countries where communications are not monitored. This is hard to fix without political will in the EU.
5. Wildcard properties exist in the implementation of the e-Commerce directive, connected to injunctive powers that district sheriffs still have. This can be solved by clarifying the instances under which injunctions can be made, and restricting the issuing authority to courts.

Together Iceland's key strengths form a very sound basis for the expansion of ICT in Iceland, especially cloud hosting. Most of the weaknesses in Iceland's position are either structural weaknesses common amongst all EU member states or are relatively trivial issues which can be resolved easily. In our model of Iceland, we have focused on the industrialized area of the country in the region around Reykjavik.

Energy

Energy is the largest cost center for most cloud hosting companies. Beyond the price per kilowatt hour, hosting companies must consider redundant network availability, power grid resilience, environmental sustainability, climate, and equipment cooling requirements as core parts of their energy strategy.

For our country data, in addition to various more specific sources, we have worked from Iceland's national energy plan, last updated in November of 2011. Based on the model for energy described in the next section, Iceland scores 3.83 out of 5.0 possible for energy.

Energy Model

We split our analysis of energy up into four main sections: energy sources, energy generation, the grid, and cooling. See the following sections for detailed analysis on each topic, and Appendix A for the rubric questions in detail.

Energy cost, reliability, and resilience is a critical driver for competitive and reliable cloud hosting. While simple cost is a very important raw metric, cheap energy on an unreliable grid is very expensive once sufficient backup generator capacity is provisioned. Likewise, for many scenarios, a single very large generation point with a single relatively reliable power intertie may actually be less appropriate than a larger number of smaller, less reliable generation points and links. All systems fail eventually, but more distributed systems are frequently more resilient, a resilience that can play hand-in-hand with decentralized cloud hosting systems.

Variability of energy pricing and availability is a critical issue for data centers, as is the renewability of power sources. The latter is especially important for hosting operations over the term of data center's useful life. Renewable power sources insulate a provider, to some degree, from fluctuations in fossil fuel market prices. Their use provides a critical differentiator within the market, and, more importantly, helps to ensure that that market will continue to exist in the future. Cheap, reliable, resilient, renewable, and predictably priced energy sources are, in combination, a significant advantage for potential hosting companies.

Examining energy pricing without examining cooling is meaningless. Estimates for data center energy utilization from IBM[1] suggest that roughly half of all energy is used on cooling, and an additional fourth on heat waste, mostly due to internal electrical resistance in system components. Therefore, a priori energy waste in typical data centers is roughly 75% before any actual computation occurs. Mitigating this waste is clearly crucial to the efficiency, cost-effectiveness and sustainability of any data center. The proportional cost of cooling for data centers has risen dramatically over the past few years, relative to the cost of hardware. Reduction in hardware deployments due to virtualization and increases in system density have dramatically reduced equipment purchase costs as a proportion of operating costs. As a result of this, component-level heat waste mitigation is a primary industry research goal.

Increasingly, large data center operators have started to look to areas with relatively cold climates. Cooling costs are significantly lower in cold areas, and most energy use in data centers in those areas that goes to cooling is attributable to airflow management and de-humidification rather than direct refrigeration. An example of this is the planned data center that Facebook, Inc., is building near Luleå, Sweden[2].

[1] https://www-950.ibm.com/events/wwe/grp/grp030.nsf/vLookupPDFs/IBM%20BladeCenter%20 Product_Tikiri/$file/IBM%20BladeCenter%20Product_Tikiri.pdf

[2] http://online.wsj.com/article/BT-CO-20111215-712478.html

Analysis of Iceland

Metric	Score
Energy Sources	
Source Renewability	5
Source Scalability	3
Supply Price	5
Energy Generation	
Generation Redundancy	4
Generation Reliability	5
Power Grid	
Grid Redundancy	4
Grid Reliability	4
Environment	
Average Temperature	5
Cold Water Availability	5
Average Humidity	2
Air Cooling Requirements	5
Freedom from Natural Hazards	4

Illustration 1: Electricity use 2009. From top to bottom: Fisheries, agriculture, general industries, district heating, home use, steel mills, services and aluminum industry. Source: Orkuáætlun 2011

Energy Sources

Electricity production in Iceland is almost exclusively from geothermal and hydroelectric primary energy sources. The theoretical maximum energy production in Iceland is 64 TWh per year from hydroelectric sources and between 10 and 30 TWh per year from geothermal sources. However, for natural protection purposes substantial regions of Iceland have been classified as natural reserves, parks, or other protected areas. In addition, certain areas have been classified as energy reserves that will not be used in coming years, in part for sustainability reasons. This lowers the effective energy available for production.

A vast amount of geothermal energy is used for house-heating (45%), followed by electricity production (39%). In addition, it is used for snow-melting, swimming pools, fish farming, greenhouses and for industrial purposes. In 2009 a total of 22.3 PJ of geothermal energy was used for electricity production.

As Iceland has little or no hydrocarbon-based electricity production, electricity prices are largely unaffected by fluctuations in the oil, gas, and coal markets, and will not be affected by supply chain interruptions in these markets. This provides a critical level of energy resilience for the Icelandic electrical system at the supply end.

Only 18% of Iceland's primary energy utilization comes from petrochemicals, of which 90% is oil and 10% coal. The majority of the coal is used by the iron smelting plant at Grundartangi, with other industrial processes consuming the remainder. Almost no natural gas is used in Iceland. Roughly 660 thousand tonnes of oil were used in Iceland in 2009, of which 41% went to powering cars, 18% for aircraft, and 29% for fishing. Petroleum use for cars has increased by 64% since 1990 in Iceland. Oil is not used for electricity production except for some emergency backup generators. Some towns have backup generators capable of sustaining basic operations throughout the town temporarily, but the redundancy of the electricity grid renders this use minimal.

Energy use for household appliances accounted for 627 GWh in 2009, accounting for 7.1 B ISK (€44.3 million) in consumer use, including VAT. Average household electricity costs in Reykjavík are 11.30 ISK/kWh, or €0.07/kWh. This rate is substantially higher than the price for industry. In the case of the aluminum smelters, these rates are 30% lower than the European average[1], although the electricity prices offered to aluminum smelting companies have been treated as confidential. Alcoa Fjarðarál reportedly paid between 28-35 USD/MWh in 2006, or roughly €0.044/kWh at 2006 exchange rates.

Despite plentiful wind in Iceland, wind power has not been developed on any significant scale.

Based on our rubric, Iceland scores 12 out of 15 possible points for energy renewability, scalability, and cost. In particular, cost of electricity is very low, and electrical power sources are more than 97% clean.

[1] http://www.mbl.is/greinasafn/grein/1026890/

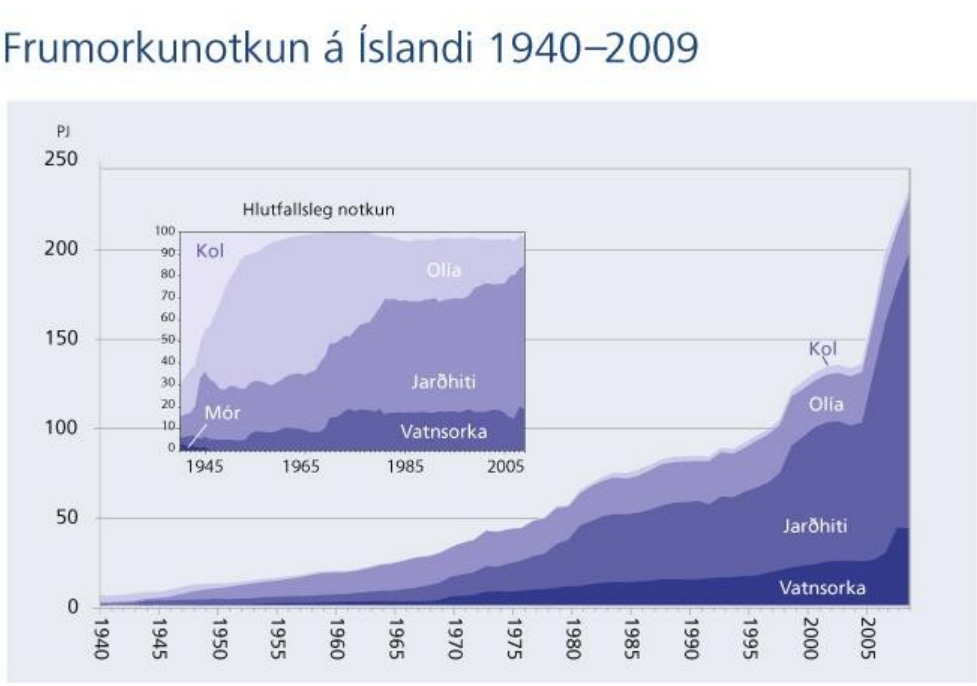

Illustration 2: Primary energy sources in Iceland 1940-2009. Inset: Proportional use.Top to bottom: Coal, oil, geothermal and hydroelectric. Source:Orkuáætlun 201

Energy Generation

In 2009, Iceland's total energy utilization was roughly 240 PJ[1] of primary energy sources, which equates to roughly 67 TWh[2]. The primary energy sources were, in order of magnitude: geothermal, hydroelectric, oil, and coal. Geothermal energy use was greater than all other energy sources combined, while coal use was relatively minuscule. Energy use in Iceland has risen substantially since the 1940's with the industrialization of the country, which up until roughly 1960 was almost entirely rural.

The current installed production capacity is 12.3 TWh per year for hydroelectric power, and 4.6 TWh per year for geothermal power. After subtracting the protected and reserve production categories, the total available hydroelectric and geothermal energy available for future expansion is 11.91 TWh per year.

There are 50 hydroelectric power stations in Iceland, mostly small. There are 7 geothermal power plants, and 4 fueled power plants—one that generates power through garbage incineration, two diesel powered, and one methane plant. The electrical production facilities have a very low incidence of outage, but one major outage occurred on September 1, 2010, leaving a significant portion of the country without power, including two aluminum smelters. A third smelter forced down to a bare minimum, however this outage - the most severe in Iceland's history - only caused a momentary interruption in power in the capital region.

[1] Petajoules. 1 PJ = 10^{15} J

[2] Terawatt hours. 1 TWh = 10^{12} W·h

In 2009, 74% of produced electricity in Iceland went to the aluminum industry, with roughly 4.9 TWh/year to Alcoa Fjarðarál, 4.0 TWh/year to Rio Tinto Alcan, and 4.0 TWh/year to Norðurál. 6% of produced electricity was used in the services industry, 5% for iron smelting plants, 5% for household appliances, 4% for utilities, 4% for general industries, and 1% in agriculture.

Based on our rubric, Iceland scores 9 out of 10 possible points for generation resilience and redundancy. In particular, power outages due to failures at power plants are very rare and generally do not affect substantial portions of the power grid.

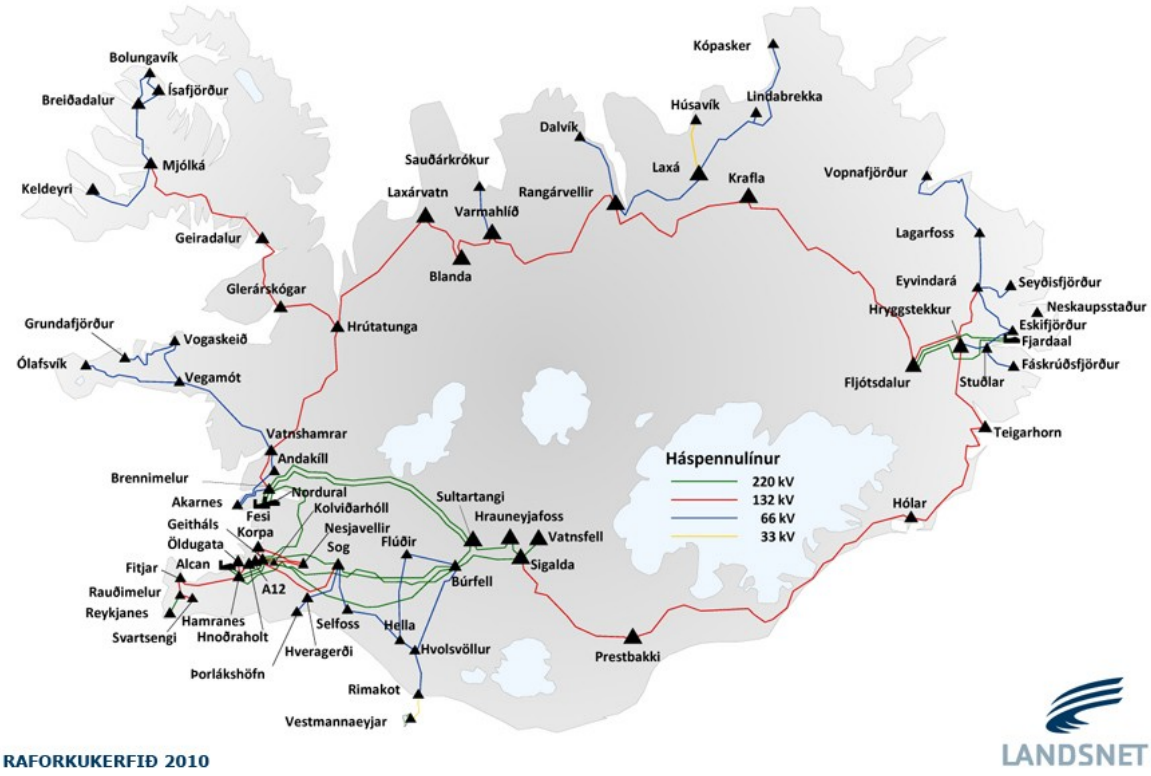

Illustration 3: Main power lines and power plants. Source: Landsnet. See also realtime energy distribution figures at http://landsnet.is/raforkukerfid/kerfisstjornun/aflflutningurnuna/

Grid Redundancy and Reliability

Power grid resilience in Iceland is fairly high. The 61 power stations in Iceland are connected with a circular grid which goes around the country, providing basic redundancy. In addition, most power stations on the southwest corner have further grid redundancy simply due to the higher population density and related network effects.

Some parts of the country, most notably the western fjords, are very poorly connected into the grid and frequently get disconnected during the winter months due to poor weather conditions. Power availability is maintained primarily with diesel generators when this happens. Similarly, Flatey and Grímsey, two populated islands off the Icelandic west and north coasts, respectively, are not connected to the main power grid, but are instead powered by diesel generators.

Resilience is quite high on the southwest corner, where most economic activity is situated, but the east coast has also improved substantially in recent years due to developments in relation to the Kárahnjúkar dam project and the Alcoa Fjarðarál aluminum smelter.

The overall infrastructural elasticity on the power grid is high enough to handle most types of outages due to line failures, power station shutdowns and disasters. Some very extreme edge cases exist where grid resilience is threatened, notably sudden outages in production units such as Kárahnjúkavirkjun, which could potentially lead to chain reactions of failures, similar to the power outage at Itaipu power station in Brazil on 21 January, 2002. In general, larger plants require larger transmission lines and inevitably cause more widespread damage when they do fail. Similarly, larger consumption units may threaten grid resilience. For instance, almost one third of Iceland's total electricity consumption is used by a single aluminum smelter, meaning that the unlikely edge case of an abrupt total disconnect would momentarily increase the available electricity substantially. This kind of pathological outage may however be mitigated by various means, not least the further diversification of power production and consumption. Based on our rubric, Iceland scores 8 out of 10 possible points for grid resilience and redundancy.

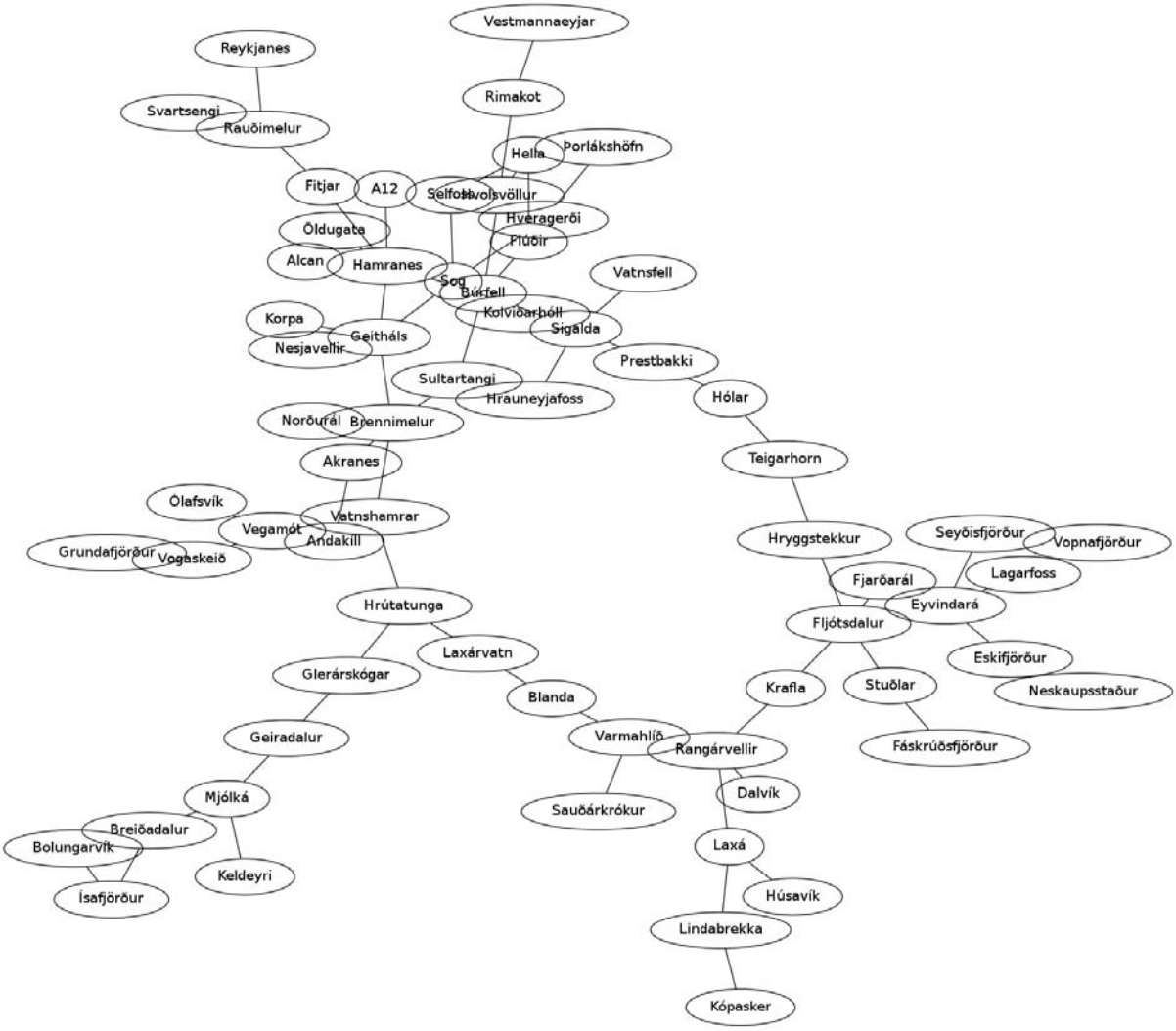

Illustration 4: A connectedness graph of the Icelandic power grid.

Environment

When examining cooling, Iceland's climate is clear benefit for cloud hosting providers even though it’s not nearly as cold as some more northerly locales. The oceanic climate contributes to relatively stable temperatures over the year. Apart from insulation, there is relatively little seasonal variation in the factors that contribute to data center cooling. On the negative side, Iceland’s climate is generally rather humid, with an annual average of roughly 70.75%. In order for outside air to be used for cooling purposes some dehumidification is needed.

Insulation averages at roughly 2.03 kWh/m²/day annually. Insulation can be useful in that it allows for solar energy production, but there is strong correlation between increased insulation and increased temperature. The average annual temperature throughout Iceland is roughly 2.94°C. In particular, the coastal regions tend to be hotter and more humid, whereas inland regions tend to be less humid and colder. Of particular interest is the Skagafjörður area in the north, which has particularly low average humidity while being relatively close to populated areas.

Due to the low temperature, the power usage effectiveness (PUE) value in Iceland is very low. PUE, as defined by The Green Grid Consortium, measures total facility power as a fraction of IT equipment power. If a facility uses no power for other purposes than the provision of computation, the fraction is 1.0, which is the ideal value. In real data center scenarios it is not uncommon for data centers to have PUE levels up to 14, meaning that for every kilowatt of power going into the operation of IT equipment, 13 kilowatts are being used for cooling, dehumidification, lighting and other purposes.

One Icelandic data center, GreenQloud, reported a PUE of 1.1, suggesting a near optimal PUE, while Verne Global suggests an operational PUE of 1.2.

A large amount of fresh water is available in Iceland, with current estimates of roughly 609,319 cubic meters of freshwater available, second only to Greenland and French Guyana. A substantial amount of this fresh water is locked in glaciers, which have been receding over recent years due to global warming. This means that there is absolutely no foreseeable water shortage in Iceland in the coming century.

Another environmental factor is natural disasters. Iceland is a very volcanically active country, sitting on a hotspot where the Earth's crust is particularly thin, and on the North Atlantic ridge, where the country itself is being ripped apart at a rate of roughly 2cm/year. This means that volcanic eruptions and earthquakes are common. In addition, Iceland's weather is extremely ferocious, with severe storms all throughout the winter, often causing avalanches in mountainous regions, such as in fjords. However, the weather is of little concern in the lowland regions, such as the south coast or Reykjanes peninsula.

Despite this, or perhaps because of this, Iceland's infrastructure has been developed to be highly resilient to environmental activity. Most settlements are outside the most volcanic areas, although they are sometimes nearby. Notable exceptions exist, such as Vestmannaeyjar, where an eruption started in the outskirts of the town in 1973. And while it is entirely possible that a volcanic eruption could occur in most of Iceland's populated areas, it is a very low probability, low frequency risk. A greater risk from volcanic activity comes from poisonous gases and ash clouds. Over an 8 month period from 1783-1784, the Lakagígar eruption spewed sulfur dioxide and hydrofluoric acid into the atmosphere, killing around 50% of the livestock and, directly or through famine, 25% of the country's population. The eruption also caused significant cooling of the northern hemisphere, in particular in Europe, where the eruption is thought to have contributed to the French revolution of 1789. A substantially less severe eruption was the Eyjafjallajökull eruption of 2010, from which ash grounded airplanes throughout Europe for several weeks. While these are severe cases, they should not pose any significant threat to a well designed data center, or to the power grid.

The electricity production and distribution infrastructure has been developed in such a way that it is not particularly vulnerable to earthquakes, although temporary power outages have occurred in relation to larger earthquakes, such as the roughly 6.5M earthquakes on the south coast of Iceland in June 2000.

Based on our rubric, Iceland scores 16 out of 25 possible points for cooling and environmental suitability. In particular, Iceland's substantial supplies of cold fresh water and its near optimal PUE values support the high score in this category.

Variable	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Average temp. °C	-2.60	-2.59	-1.59	1.37	5.24	8.49	10.31	9.58	6.29	2.75	-0.04	-1.91
Insolation, kWh/m²/day	0.11	0.53	1.31	2.77	4.11	4.71	4.16	3.27	2.17	0.97	0.25	0.03
Wind speed, m/s	10.20	10.27	9.63	8.42	7.18	6.51	6.40	6.63	7.62	8.85	8.76	10.41
Humidity, %	80	78	71	69	66	66	63	61	67	72	77	79.0

(Reykjavík average temperature, insolation and windspeed, source: Gaisma.com)

Connectivity

Good connectivity to Internet is fundamental for enabling cloud service provision. Many factors play a part in connectivity, such as bandwidth, latency, network redundancy, scalability and system security. Good connectivity is not decided by any one single factor, and in many cases one factor can be non-contributory to a good network, depending on the purpose and use model for the network.

Based on the model for connectivity described in the next section, Iceland scores 3.58 out of 5.0 possible for connectivity.

Connectivity Model

The connectivity model is split into domestic connectivity, and then different areas of the globe. As is true for true for all parts of the model, the domestic connectivity model must be focused on the region that is relevant for hosting. See the following sections for detailed analysis on each topic, and Appendix A for the rubric questions in detail.

The connectivity model for domestic networks is a superset of the model used for each area of the globe. The composite score for connectivity to each area is averaged in with the primary model as a single line item. The domestic network section contains a number of additional items that are relevant for all connectivity within (and in some cases, merely transiting) the country.

The basic set of measures, common for both domestic and global network links, covers the resilience of the network, in terms of redundancy and reliability, it's current capacity, in terms of both latency and throughput, and how able the network will be to scale up, both in terms of scaling with existing installed capacity and with existing plans to install new capacity. The general items added to this look in more detail at the resilience of the network, with specific regard to emergency response and security issues.

Capacity of a network, both for domestic and global data transmission, is a basic qualifying factor for hosting cloud services; if the capacity is not available, with room to grow over time, it's not possible to provision service regardless of how desirable a location may be for hosting in other respects. However, resilience is being recognized as an increasingly critical issue for large-scale hosted systems, where network downtime may be measured hundreds of thousands or even millions of euros per hour. As networks become increasingly contested from a security perspective, the security response of the Internet within a given country will become increasingly important as well.

Analysis of Iceland

Metric	Score
Domestic Connectivity	
Redundancy	4
Reliability	5
Scalability	4
Throughput	3
Latency	5
Expansion	3
CERT Responsiveness	2
DDoS Outage Frequency	5
Targeted Attack Incidence	2
Central/Western Europe	
Redundancy	4
Reliability	5
Scalability	5
Throughput	5
Latency	3
Expansion	5
North America	
Redundancy	2
Reliability	5
Scalability	5
Throughput	3
Latency	3
Expansion	5
Eastern Europe/Russia	
Redundancy	1
Reliability	5
Scalability	5
Throughput	3
Latency	2
Expansion	5
MENA	
Redundancy	1
Reliability	5
Scalability	5
Throughput	2
Latency	2
Expansion	1
East/South-East Asia	
Redundancy	1
Reliability	5
Scalability	5
Throughput	2
Latency	1
Expansion	2

Domestic Connectivity

The main domestic telecommunications hub is RIX (Reykjavík Internet Exchange), which is operated by ISNIC. Founded in 1999, this hub connects the main Internet service providers and data centers together. While the hub constitutes a single point of failure, some networks have alternative routing between each other and many have their own international uplinks, both of which increase redundancy. Relatively few system outages have had widespread effects on the domestic network. Outages tend to be localized and very short term.

Domestic fiber optics and copper networks are operated by Míla, Fjarski and Gagnaveita Reykjavíkur. Míla is a subsidiary of the formerly state-run phone company (since privatized, currently known as Síminn). It operates a fiber optics ring around the country which were installed by NATO, but has expanded it substantially and introduced additional redundancy. It also operates fiber and copper networks in most settlements. Fjarki is a subsidiary of Landsvirkjun, the mostly state owned power company. Gagnaveita Reykjavíkur is a subsidiary of Orkuveita Reykjavíkur, the Reykjavík city power company. It provides mostly fiber to the home connections but also operates some communications backbones within the Reykjavík metropolitan area.

In the capital region, redundancy is rather high and network availability is good, however the infrastructural elasticity drops when outside the southwest corner. The fiber rings guarantee a very low risk of a countrywide outage, but many regions, such as the Westfjords, are poorly connected into the larger network.

Based on our rubrics, Iceland's domestic network gets a score of 3.66 out of 5. In particular, the domestic network's heavy reliance on fiber optics all the way to the home or office, as well as low incidence of network security issues contribute to a good overall domestic score, although targeted attacks on the network infrastructure are relatively commonplace, they are mostly ineffectual. These aspects will be covered in more detail in the network security section below.

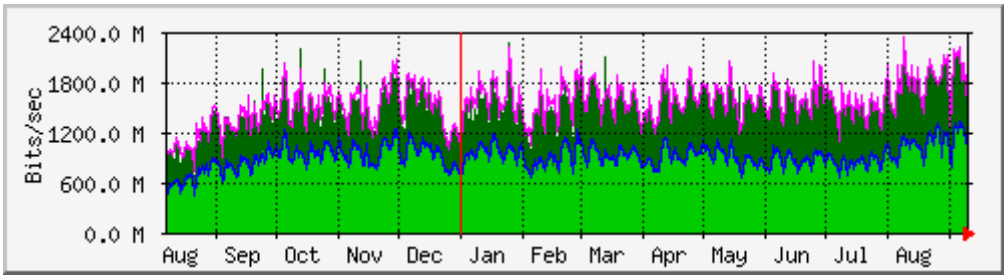

Illustration 5: RIX total bandwidth over a one year period. Source: RIX, September 2012.

Connection speed	AS number	Network
10G	1850	Internet á Íslandi (ISNIC)
10G	15474	Rannsókna og háskólanetið
10G	6677	Síminn
10G	2603	NORDUnet A/S
10G	12969	Vodafone
10G	43892	Basis
10G	25509	Hringiðan
10G	24743	Snerpa
10G	29348	FSnet
10G	31236	Reykjavíkurborg
10G	25152	RIPE NCC K-root server
10G	31441	Gagnaveita Reykjavíkur
10G	31410	Netsamskipti
10G	39472	Arion Banki hf.
10G	44515	EJS ehf.
10G	26415	VeriSign Netherlands B.V.
10G	51896	Hringdu ehf.
10G	44735	Símafélagið ehf.
10G	44432	Backbone ehf.
10G	43571	NOVA ehf.

Table 1: Networks connected to RIX

International Connectivity

Iceland's connectivity to the outside world has improved substantially over the last two decades. Since 1994, submarine fiber optics connections have existed to the Europe and North America. Since 2004, domestic Internet connectivity has gone up from 81% of households to 90%, compared to EU growth from 41% to 65%. Of the 10% of Icelandic households not connected to the Internet, 40% (4% of the total) claim not to want an Internet connection, whereas 25% (2.5% of the total) say it is due to price of connectivity.

As of November 2011, there are four fiber optics cable links to Iceland: DANICE, Greenland Connect, FARICE-1, and CANTAT-3, in order of decreasing capacity. Several projects have been proposed to increase the number of fiber optics links to Iceland; of them, Emerald Express is the furthest towards completion.

The CANTAT-3 was the first fiber optics cable connection to Iceland, greatly increasing the country's telecommunications capacity. Installed in 1994, it was disrupted in late 2006 and was not returned to full capacity until mid-year 2007. The CANTAT-3 cable was retired in late 2010, due to age, operational costs, and low capacity.

Farice ehf. operates two fiber-optic submarine systems as of late 2011. It is partially owned by the Icelandic state and Arion bank, but a 20% stake is held by Faroese shareholders.

Their first system, FARICE-1, lies between Seyðisfjörður, Iceland and Dunnet Bay, Scotland with a layover in Funningsfjørður in the Faroe Islands. From these locations it is backhauled to Reykjavík, Edinburgh and Tórshavn respectively. It traverses a roughly 1,400 km route using Dense Wavelength Division Multiplexing (DWDM) transmission technology. It has been in use since 2004 and is currently Iceland's main communications line. Currently only roughly 3% of FARICE-1's total potential capacity is installed, according to available sources.

Farice ehf.'s second system, DANICE, was laid in 2008 and connects Landeyjarsandur in Iceland to Blaabjerg, Denmark, with a planned expansion to Eemshaven, Netherlands. Despite having significantly greater capacity than FARICE-1, it is much less utilized and mostly used as a redundancy cable for FARICE-1.

The most recent fiber optic connection to Iceland is through Greenland Connect, installed in 2009 and owned and operated by TELE Greenland. It connects Milton, Trinity Bay, Newfoundland and Labrador, Canada, to Nuuk, Greenland, Qaqortoq, Greenland, and Landeyjarsandur, Iceland. It contains two fiber pairs specified for 128 wavelengths carrying 10 Gb/s each. As its landing point in Iceland is co-located with the DANICE cable, direct bridging between them is possible.

The Emerald Express is a planned 6x100x100 Gb/s fiber optics cable from the United States to Ireland with an offshoot to the Reykjanes peninsula in Iceland. Being constructed by Emerald Atlantis, Ltd. and TE SubCom, Ltd., it is scheduled to enter service in late 2012 and intends to facilitate ultra-low-latency connections to Europe and North America.

Fiber optic cable	Owner	Total capacity	Current capacity	Comment
CANTAT-3	Síminn	7.5 Gb/s	None	Decommissioned
FarIce	Farice ehf	720 Gb/s	Unknown	
Danice	Farice ehf	5.200 Gb/s	~20 Gb/s	
Greenland connect	TELE Greenland	1.900 Gb/s	Unknown	
Emerald Express	Emerald Networks	58.600 Gb/s (planned)	N/A	Under construction

Table 2: Fiber optics cables to Iceland

Its Iceland branch will presumably carry two pairs, one for connection to Ireland, the other to the United States; the last pair connecting the US to Ireland directly.

Total capacity of installed fiber optic cables is currently around 7.8 Tb/s, not counting the CANTAT-3 cable. However, endpoint equipment has only been installed for a fraction of this capacity. The installed capacity is not known, but conservative estimates put it close to 200 Gb/s, or around 2.5% of the total capacity.

Current utilized capacity is also unknown, but various estimates can be used to arrive at a figure. The combined foreign connectivity of universities and secondary colleges in Iceland is currently 16.5 Gb/s through RHNet. As RHNet typically accounts for between 14.2%-14.9% of total traffic through the Reykjavík Internet Exchange, it can be estimated that total foreign bandwidth consumption is close to 120 Gb/s.

Uplink redundancy to Europe is good due to the FARICE-1 and DANICE cables going separate routes. However, redundancy to the US is poor, since the only reliable connection is through Greenland. Currently, in the case of an outage, rerouting would have to be through Europe —presumably London. US redundancy will improve substantially when the Emerald Express is completed.

Overall uplink redundancy is becoming better, providing more infrastructural elasticity and greater resilience. The older emergency satellite redundancy is slowly becoming less relevant and is probably not realistically needed. Round-trip latency to Europe is generally low, but varies widely depending on destination city and provider, origin location and provider, and various other variables. Generally speaking the network latency has low stochasticity ("jitter"), averaging around 4ms (milliseconds), suggesting natural latency[1] rather than network congestion.

We did informal testing of multiple origin and endpoints on known locations to arrive at some idea of latency trends. Typical round-trip times to London are close to 55ms; 31ms to Copenhagen. Connections to Oslo trend around 70ms, Berlin around 71ms, and to Madrid 74ms. On connections closer to the uplinks, slightly better times were observed, while household Internet connections showed slightly worse round-trip times. As such, none of this was particularly unexpected.

[1] Natural latency is latency attributable to physical attributes and limitations in the channel and equipment under optimal circumstances rather than latency due to network congestion.

The theoretical round trip time for a photon traveling over the big circle route from Reykjavík to London is 12.64ms; to Copenhagen it is 14.02ms. Therefore the Copenhagen connection is as close to reasonable expectations as is possible, while the London connection could possibly be improved. The FARICE-1 endpoint is in Edinburgh, so packets bound for London must traverse potentially congested and slow UK networks after their initial arrival.

As seen, connectivity to Central- and Western Europe is quite good, and connectivity to North America is decent. Plans for the expansion of these are rather extensive, and with future developments on various stages, as discussed in more detail below, promising to provide greater connectivity to North America and Western Europe, as well as Russia and potentially East Asia. Resultingly, based on our rubrics, Iceland scores 4.5 in connectivity with Central- and Western Europe, 3.83 in connectivity with North America, 3.5 in connectivity with Eastern Europe and Russia, 2.66 in connectivity with the Middle East and North Africa, and 2.66 in connectivity with East and Southeast Asia.

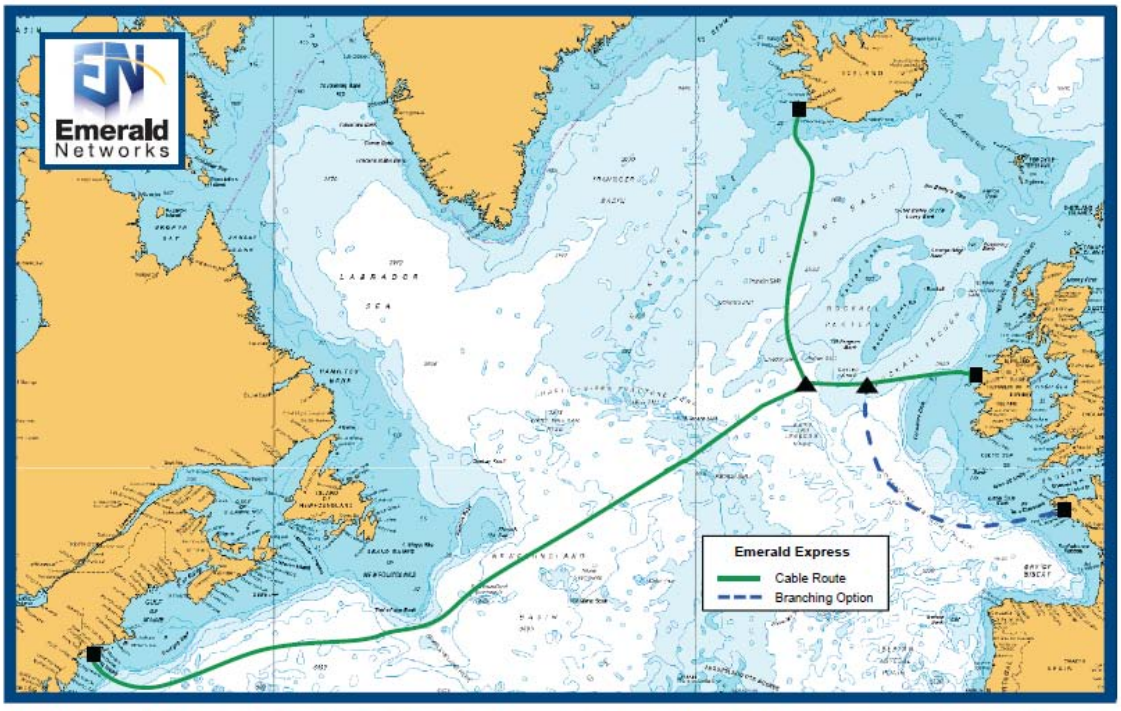

Illustration 6: Map of proposed Emerald Express cable. Source: EmeraldNetworks

Network Security

No major network security incidents have occurred in Iceland. Denial of Service attacks happen on a relatively small scale on a fairly regular basis, but are easily mitigated with standard techniques. No large scale online attacks have occurred in recent years, although in some cases competent attackers have been able to disable individual service providers for a number of hours. This is not considered to be more frequent in Iceland than in the EU.

Individual servers and home computers are moderately well protected from security threats compared to other countries, owing to a fair degree of awareness, a comparatively low incidence of pirated operating system software, and generally well configured routers on home connections. That said, many computers run outdated operating systems with severe security vulnerabilities, and many websites operate outdated web platforms, in particular Wordpress and Joomla, which are common staging grounds for attack.

The Icelandic government is acutely aware of the threats posed to the security of networks, and in recently proposed amendments to the telecommunications act, provisions are made for the establishment of a CERT (Computer Emergency Response Team). This should increase multi-party coordination and responsiveness in the case of online attacks or other ICT-related emergency, and thus overall communications resilience.

Illustration 7: Example routes for a "polar express" cable; also shows autumn arctic ice cover. Image generated with Google Earth.

Future Connectivity Developments

A number of proposals have been made for future developments in connectivity in Iceland.

One example which has frequently been brought up is that Iceland's geographical situation makes it ideal for connecting the American east coast, Europe, and East Asia, due to the receding polar ice cover. Such a connection could land in Longyearbyen in Svalbard, and have connections to Murmansk, some settlements along northern Siberia, and either connect to Yakutsk via the Lena river or go through the Bering strait and connect to Alaska on the one hand and Kamchatka and Japan on the other hand.

This would shorten round-trip latency to East Asia substantially, as most current connections go through the Mediterranean, down past India, and through the South China Sea. The Longyearbyen connection would allow for redundancy to Norway through an existing connection. Connections in Russia would help in Russia's developing ICTs, as currently it is estimated that 70% of Russian communications go through Sweden. However, it would be vital to Europe's communications security interests that such a connection have direct routes to East Asia rather than an intermittent landing in Russia. There are numerous ways in which such a proposal could be made beneficial to all parties, and it would open possibilities for diverse applications from cross-continental high speed trading and currency arbitrage to online gaming. For telephony applications, this connection would push the latency on communications between Europe and East Asia down below the threshold of human perception, itself a revolution in global telecommunications.

Less ambitious potential developments that have been proposed include construction of large data centers on the Reykjanes peninsula, construction of further fiber optics links to Europe and America, and the establishment of data caches and mediation centers in Iceland for high availability applications. With this in mind, Hibernia Atlantic has been considering options for a low latency cable to New York.

Illustration 8: ROTACS and Arctic Fiber. Source: Laser Focus World

Jurisdiction

Core to any economic venture in modern societies is the jurisdiction in which they are conducted. Variations in jurisdiction can alter the cost structure of service provision quite substantially - from state security burdens such as surveillance, data retention, censorship or key escrowing to simple issues of taxation and access to qualified people on the job market, any number of things can effect the viability of a legal jurisdiction for the hosting of data centers or cloud services.

In our model, we aim to provide a comprehensive overview of the issues regarding jurisdiction. Our analysis of Iceland gives the country an overall score of 3.70 out of 5 in the jurisdiction category.

Jurisdiction Model

As with the other sections, our jurisdiction model is divided into a number of high-level categories. See the following sections for detailed analysis on each topic, and Appendix A for the rubric questions in detail. Unlike other sections, all elements in this part of the model apply to the country as a whole.

Some jurisdictional issues are basic requirements for implementing cloud hosting in a country, such as an available qualified labor pool and the basic requirements for doing business with outside entities, but most of the issues here are, similar to connectivity and energy, shaping the desirability and profitability of a jurisdiction.

Security burdens represent an especially troubling area, as not only can the costs a provider is forced to bear be significant, but some burdens here may effectively compromise the security of the rest of a provider's network, and, especially in systems that do not geographically segment the hosting of user data, effectively compromise the privacy of all users of a system. Likewise, the competitive landscape of a country has the possibility to pose an existential threat to the operations of a provider, when liability limitations and software patents are in play.

On the other hand, commercial issues like tax rates and capital restrictions mostly influence final profitability. Legal issues fall somewhere in between -- an unfavorable legal environment may render a jurisdiction too complicated to deal with, especially if a great deal of uncertainty or a legal system with a significantly different operating basis is at issue. Human resources are a basic capacity question for hosting, similar to available network bandwidth, although favorable immigration policies can help here.

Analysis of Iceland

Metric	Score
State Security Burdens	
Surveillance Burden	4
Censorship Burden	4
Data Retention Burden	3
Key Escrow Burden	5
Network Militarization Burden	5
Competitive Landscape	
Software Patent Burden	5
Anti-Monopoly Protection	4
Libel Tourism Protection	4
Carrier Liability Limitation	5
Intermediary Liability Limitation	5
Network Neutrality	3
Takedown Notice Regime Burden	4
Commercial Issues	
Capital Restriction Burdens	1
Currency Market Size	1
VAT Burden	1
Equipment Import Duty Burden	3
Service Provision VAT Burden	1
Corporate Tax Rate Burden	3

Metric	Score
Legal Friction	
Incidence of Sanctions	5
Legal Stability	4
Strength of Rule of Law	5
EU Directive Compatibility	4
Human Resources	
Availability of Qualified Workforce	1
Average Wage Burden	4
Social Welfare Burden	4
Immigration Flexibility	5
Language Compatibility	5

Iceland is a parliamentary republic which gained independence from Denmark in 1944. It is a member of the United Nations, the Council of Europe (CoE), the European Economic Area (EEA), the European Free Trade Association (EFTA) and the North Atlantic Treaty Organization (NATO), amongst others. It is party to numerous international agreements including Schengen.

Iceland's membership in the EEA means that outside of a few limited areas, all EU commercial directives take effect in Iceland. In addition, both for conformity and utility, Iceland has adopted various non-EEA relevant directives. This tendency has been increasing as part of the preparations and negotiations for EU membership. As of 12 December, 2011, eight out of 33 chapters have been closed in Iceland's EU accession negotiations. Of particular interest to this report, the chapter on information society and media is considered to generally already conform to the EU acquis.

State Security Burdens

The Telecommunications Act (Law 81/2003) was amended in 2005 to include provisions for data retention. It applies to telecommunication providers and its current implementation mandates the retention of records of all connection data for 6 months. It states that communications companies may only deliver information on telecommunications in criminal cases or on matters of public safety. It also states that such information may not be given to others than police and public prosecution.

According to COM(2010) 62, an analytical report accompanying the communication from the Commission to the European Parliament and the Council containing the Commission Opinion on Iceland's application for membership to the European Union, Iceland has not currently implemented the Data Retention Directive. This directive is currently being discussed (December 2011) in the Icelandic Parliament, however there are complications owing to the fact that the Data Retention Directive, 2006/24/EC, came into effect one year after the Icelandic Data Retention provisions, which have not since been overturned or amended. However, the 2005 law which established data retention in Iceland was made at the request of the Icelandic police chief (Ríkislögreglustjóri), making use of the current discussions that were then ongoing in the European Commission about the issue. Therefore, the implementation of data retention is structurally equivalent to the data retention directive, although formally the EU directive has not been implemented.

During discussions in the Icelandic parliament about the (formal) implementation of the data retention directive, some parliamentarians were surprised to find that such a broad surveillance law already existed in the telecommunications act. There have been discussions, both public and within the parliament, about the potential abolition of data retention. However, this would impede the EU membership process and is therefore unlikely to gain traction without any political support from within the EU.

There is an ongoing discussion about granting police enhanced surveillance rights, in the form of proactive investigative measures aimed at counteracting organized crime and terrorism. Although these measures have not yet been implemented, there is currently a resolution proposal being processed in the parliament. The interior minister, Ögmundur Jónasson, has independently stated that he is preparing proposals for such a law. The scope of such a law is unknown, but it is clear that proactive investigation measures would necessarily have to include expanded rights for telecommunications surveillance.

Wiretapping and other electronic surveillance is regulated under the Telecommunications Act (81/2003) and further defined in Rules no. 837/2006 on Electronic Surveillance

Both data retention and surveillance support add to operating costs and jurisdictional uncertainty for cloud hosting providers, especially given the complexity of unsettled international cross-jurisdictional issues.

As of June 2012, a CERT team has been established by law in Iceland. The law contains provisions for allowing the CERT team to perform limited surveillance of a computer network, having been granted permission to do so by the network operator. It also gives the CERT team the right to report illegal activities on the network to the police. This combination could potentially be abused as a gateway to blanket surveillance, as has been noted in a memo issued by the Icelandic Digital Freedoms Society^[Full disclosure: one of the authors of this report, Smári McCarthy, co-signed the memo in question and is a board member of the Icelandic Digital Freedoms Society at the time of writing.], but with greater restrictions (such as a ban on deep packet inspection and identification of individual users or network analysis that could compromise a user's identity), it could serve to improve network security.

No state censorship is currently practiced in Iceland.

Corporate censorship has been employed by telecoms providers in a few cases, at request of police and child protection authorities. Most notable was the anonymous forum site Ringulreið, which was accused of being a center for cyber-bullying. After the major telecoms providers, Síminn and Vodafone, voluntarily censored access to the site from its users, the site was shut down by its operators.

Some ISPs, most notably Síminn, the largest ISP in Iceland (formerly the state telecoms company) offer parental filtering services to their customers on an opt-in basis. Such blocking software is largely controlled by end-users, although it is somewhat unclear by which criteria websites are added to these filter lists. However, no anti-competitive, political or religious censorship has been noticed in these systems. Recently, both Síminn and Vodafone have proposed to adopt such systems generally on an opt-out basis, specifically targeting pornography and gambling sites, under the assumption that this will improve network security.

Over the last year, it can be argued that abuse of libel law has been on the rise. Journalists and commentators have been increasingly found guilty of libel for comments made on online media. In particular, one journalist has been found guilty for directly quoting an interviewee, whose statement was considered to be libelous by the court. In another case, an elderly woman was found guilty of libel for a Facebook comment wherein she made a value judgement on the characters of the claimants. Of course, in each of these cases there are competing interests and some uncertainty left to the courts, but many have commented on the potential chilling effects associated with such lawsuits and have called for reform.

No key escrowing is conducted in Iceland. Iceland has no military, and is not engaged in any form of military buildup, electronic or otherwise.

Competitive Landscape

Iceland's competitive landscape is relatively good. In particular, there is no legal basis for software patents in Iceland and there are relatively good protections for telecommunications intermediaries[1].

Law 30/2002 on e-commerce and electronic services implements the e-commerce directive (2000/31/EC), which provides indemnity for "mere conduits", such as telecommunications networks and Internet hosting providers.

There are few and mostly well defined exceptions to this indemnity:

1. an injunction from a sheriff or court order
2. a notice-and-takedown procedure regarding copyright infringement
3. knowledge of child pornography

The exception for general court orders without further definition is worrying, due to the remnants of an magistrate system mostly abolished in 1991. Prior to this, the district "sheriff" (sýslumaður) also served as magistrate and had the ability to, amongst other things, enact injunctions. When their magisterial rights were revoked with the 1991 law, they retained their ability to enact injunctions. Although this has not caused problems in terms of Internet hosting, a sheriff's injunction was used in 2009 to prevent the state broadcaster, RÚV, from airing a story pertaining to a leaked large loan book from the bank Kaupþing. As the injunction was revoked when the injunction had failed, it was never taken to court, so its veracity under the constitution was not tested.

The exceptions should probably be improved by clarifying which exact circumstances can trigger such exceptions, as well as restricting the injunction measures to actual courts.

There is no law in Iceland guaranteeing network neutrality. Networks are mostly neutral, although the large phone companies, Síminn and Vodafone, have engaged in limited blocking and filtering.

As a signatory of the Lugano treaty, Icelandic courts can decide not to uphold foreign court verdicts which go against the rule of law in Iceland. This means that a libel verdict from a foreign country can be challenged in an Icelandic court on the basis of article 34 of the Lugano treaty if it comes from a country with a substantially different burden of proof for libel than Iceland does. This has not been tested in practice, but could serve as a basis for protecting Icelandic citizens in cases of so-called libel tourism.

[1] In the comparative model, a distinction is made between carriers who simply mediate data through their networks, and intermediaries who perform more complex network activities.

Commercial Issues

After the collapse of the Icelandic banking sector in 2008, the Icelandic Central Bank (Seðlabanki Íslands) was authorized to put limitations on the flow of capital, in particular those with no relevance to goods or services. The Central Bank is also authorized to require domestic companies to deposit and exchange foreign currency. As of November 2009 all restrictions have been lifted on new investments, and in practice trade from Iceland is not hindered substantially by the capital restrictions.

VAT in Iceland is generally quite high, with most goods and services falling in the 25.5% VAT category. However, law 163/2010 introduced new exceptions to the VAT law (law 50/1988) which makes data processing and information provision, as well as "electronically provided services" exempt from taxed capital flows.

Further, this law allowed an exemption from VAT for the importation of servers and related equipment (i.e., equipment which is necessary for the functioning of the servers and is only of direct benefit to the owners of the servers) in cases where the owners have official residence in other member states in the EEA, EFTA, or the Faroe Islands, and do not have fixed operations in Iceland in accordance with Icelandic tax law.

This exception puts more specific requirements, for example that the owners of the servers pay VAT in their home country, that the purpose of the operations be of such a nature that it would require commercial registration if it were domestic, that the servers were imported specifically for the purpose of operation in a data center which their owner is in business with, that the servers and other equipment are used only by the owners, but not for other purposes within the data center, and that the servers be used from outside of Iceland. This exception is due for reconsideration in late 2013, but as it stands is exceptionally beneficial for cloud hosting providers.

Overview of Icelandic Information Regulation

Icelandic law conforms broadly to the European *acquis* regarding a number of different information regulations.

Telecommunications are in general governed by law 81/2003 (telecommunications act), which implements EU directive 999/5/EC, regulation 2887/2000/EC, the Telecoms Package (directives 2002/19/EC, 2002/20/EC, 2002/21/EC and 2002/22/EC), and directives 2002/58/EC and 2002/77/EC.

Electronic commerce and other electronic services are generally governed by law 30/2002, which implements the e-Commerce directive (2000/31/EC), thereby establishing intermediary liability limitations which are crucial to the functioning of Internet service providers, hosting providers and data centers. The only practical failing of the Icelandic implementation of the e-commerce directive is that allowance is made for injunctions which, for historical reasons, can be issued by a regional sheriff (*sýslumaður*) without court supervision. This has not caused problems in the context of intermediary liability limitations, but has been used to stifle media on one occasion, and could potentially be abused further.

Media is regulated under the media law, 38/2011, which implements Audiovisual Media Services Directive (2007/65/EC). Broadcast media is also regulated by the telecommunications act (81/2003).

Personal and private data is protected under law 77/2000, which implements the Data Protection Directive (95/46/EC).

Electronic signatures are allowed as a valid form of signature under law 28/2001, and to this end a national authentication card scheme has been developed and is being distributed as a feature of banking cards.

Freedom of access to government information is defined in law 50/1996. This law has been under review, and a broad-reaching proposal for a new freedom of information law was submitted to the Parliament during its 139th term (ending in October 2011), but did not make it through the parliamentary process before the end of the session. A small subset of the changes proposed in that law by the relevant parliamentary committee were adopted into a new version of the bill which was submitted to parliament at the beginning of the 140th term. This new version did not include provisions proposed by the review committee regarding public registration of government documents and public advertisement of confidentiality terms, reasons and durations for secret documents. The bill has been proposed for the third time at the 141st parliamentary term, with little changes.

With regard to intellectual monopoly rights, patents are defined in law 17/1991, biopatents in law 58/2000, descriptions of electronic components are protected under law 78/1993, trademarks under law 45/1997, and in particular corporate logos are protected under law 155/2002. Finally, copyrights are defined in law 73/1972, which implements EU directives 89/552/EEC, 2003/4/EC, 2001/29/EC, 2001/84/EC, 91/250/EEC, 92/100/EEC, 93/83/EEC, 93/98/EEC, 2004/48/EC (IPRED)

and 2006/123/EC. Law 53/2006 defines specific permissions regarding the collection of evidence pertaining to violations of intellectual monopoly rights.

Compatibility with European Union Directives

As previously stated, Iceland's laws regarding information technology and media are largely in accordance with European *acquis*. However, in the European Commission's Opinion on Iceland's application for membership of the European Union (COM(2010) 62)[1], a few minor issues are laid out.

The most salient issue is that the EU Data Retention Directive (2006/24/EC) has not been transposed. This is however a trivial issue——the telecommunications act contains provisions for data retention which originate from early drafts of the data retention, and is in all regards equivalent to the Data Retention Directive. Therefore, transposition is a formality. Data retention will be discussed further in the later section on electronic surveillance.

Also according to the opinion, while "the legislative and administrative structure is similar to most EU Member States" the appointment procedures for the national regulatory authority (the post and telecoms administration, *póst- og fjarskiptastofnun*) have to be revisited to ensure transparency, objectivity, and high standards regarding security of tenure.

It goes on to say that "in the field of information society services, the main directives have been transposed into the Icelandic legal order, i.e. the Directives on electronic signatures, e-commerce and conditional access."

[1] http://ec.europa.eu/enlargement/pdf/key_documents/2010/is_opinion_analytical-report.pdf

Data Protection

Data protection is regulated under law 77/2000, which implements EU Directive 95/46/EC (Data Protection Directive) and parts of EU Directive 97/7/EC (Equal Treatment in Social Security Directive). The day-to-day management of compliance is managed by the Data Protection Authority.

Various rules and regulations apply with regards to data protection that might have relevance to data centers and information hosting, specifically:

1. Rules no. 837/2006 on Electronic Surveillance.[1]
2. Rules no. 698/2004 on The Obligation to Notify and Processing which requires a Permit.[2]
3. Rules no. 299/2001 on security of personal data[3]
4. Regulation no. 322/2001 on Management of Personal Information by the Police[4]

[1] http://www.personuvernd.is/information-in-english/greinar/nr/610

[2] http://www.personuvernd.is/information-in-english/greinar/nr/441

[3] http://www.personuvernd.is/information-in-english/greinar/nr/442

[4] http://eng.domsmalaraduneyti.is/laws-and-regulations/nr/1042

Human Resources

Iceland is a highly educated country. Out of a workforce of 181,000 people, 33.3% have primary education, 38.2% have vocational education, and 28.1% have university education.

After the financial crisis started in 2008, unemployment rose from 1.01% in 2007 to 8.13% in 2010. Recent reports suggest that the unemployment rate is going down, but that has not been confirmed by publicly available statistics.

A 2006 OECD report showed that the number of scientific and engineering publications in internationally recognized journals had increased at an average annual growth rate of 5.7% since 1998 and that between 1991 and 2001, the number of publications per million population increased by 50%, from 403 to 610, compared to averages of 416 and 556 in those same years in the EU15. At that time, Iceland ranked eighth in the number of citations per paper (worldwide). The financial crisis caused some reductions in innovation and research & development funding, but this primarily had the effect of shifting researchers further into private sector research operations and startup companies. On the other hand, Innovation Center Iceland has started a number of seed labs where startup companies and small proprietors can rent inexpensive office space.

Bala Kamallakharan has noted[1] that 2011 was a record year for insolvencies in Iceland, while the number of new company registrations has dropped significantly. This could perhaps be attributed to unavailability of capital available to startups, or perhaps deflation of the last decade's bubble. Without suitable employment for its highly skilled labor force to absorb, Icelanders will either resort to leaving for better opportunities abroad or remain idle domestically letting their considerable talent go to waste.

Either way, the combination of experienced researchers, high unemployment rate, low rate of startup and high insolvency rate suggests that unless Iceland continues to experience an increase in "brain drain", where well educated people seek employment outside the country, a significant underemployed or unemployed workforce will exist in Iceland.

[1] http://www.startupiceland.com/2012/01/2011-has-been-record-year-in-iceland.html

Icelandic Modern Media Initiative

On July 16th 2010, the Icelandic Parliament, Alþingi, unanimously adopted a parliamentary resolution to develop in Iceland advanced legislation for the protection of the rights to information and free speech. Since then, the Icelandic Modern Media Initiative, or IMMI, as it was called, has been in development, both inside the government ministries and institutions, and within Icelandic civil society. The originators of the IMMI initiative founded, in 2011, the International Modern Media Institute, a synacronymous civil society organization working towards ensuring that the goals and spirit of IMMI are met in Iceland, and sharing the ideas and developments with the world at large.

In this chapter we review the status of the IMMI project in its aspirational goals. Whereas most of this project's goals have not been implemented in law, they do not factor into the jurisdiction model and therefore do not factor into the analytical model at all. However, as this project may prove to be influential, a summary chapter is included. This summary chapter is partially based on IMMI's April 2012 status report, but updated to include recent developments.

Subject area	Status	Notes
Source Protection	Complete	Media law + constitution
Freedom of Information Act	Pending ratification	New law replacing older law + constitution
Communications Protection	Pending ratification	Changes to law + constitution
Intermediary Liability Limitations	In development	Changes to law + constitution
Publishing Liability Limitations	In development	Changes to law
Whistleblower Protection	In development	Changes to law + constitution
Prior Restraint Limitations	Pending ratification + In Development	Constitution + regulatory changes
Judicial Process Protections	On hiatus	
Network Neutrality	Pending ratification	Constitution
Virtual Limited Liability Companies	On hiatus	
Freedom of Expression Prize	On hiatus	

Source Protection

The protection of sources refers to measures which forbid journalists from exposing the identity of their sources without the source's permission. The purpose of such measures is to increase the willingness and security of sources who consider themselves to be at risk, when providing information of criminal wrongdoing, corruption, negligence or other socially unacceptable behavior to journalists.

Journalistic source protection was implemented in Icelandic law 38/2011 (the media act). The source protection clause is defined in article 25., which states:

> Employees of media organizations which have been licensed or registered with the media committee are forbidden to expose the identity of source for articles, books, retellings, announcements or other material, regardless of whether it has been published, if the source or the author requested anonymity. Employees of the media organization are also forbidden to release data which contain information regarding the source or author in such circumstances.
>
> The rule in the 1st paragraph also applies to those who, due to connections to the media organization or the production of the material has gained knowledge of the identity of the source or author, or has attained data to that effect.
>
> Source protection under paragraphs 1 and 2 can only be relieved with the permission of the source or the author, or on the basis of article 119 of the law on the prosecution of criminal cases, no. 88/2008.[1]

In addition to the stipulation in the new media law, the proposed constitution for Iceland contains, in article 16, the statement:

> The protection of journalists, their sources of information and whistle-blowers shall be ensured by law. It is not permitted to breach confidentiality without the consent of the person providing the information except in the process of criminal proceedings and pursuant to a court order.

This provides equivalent protection under the constitution, if ratified, ensuring that the source protection clause would not be removed from law without referendum.

[1] The exception in article 119 of law 88/2008 applies to the case where criminal proceedings for serious offences cannot be resolved without the identity of the source or author being exposed. In such cases, it has been recommended although it is not stipulated in statutes, that the identity first be exposed to the judge *in camera*, so that the judge can appropriately measure the potential risk to the source against the benefit of the source's exposure. This is generally considered an acceptable limitation to the otherwise absolute source protection clause.

Freedom of Information Act

Access to government documents and records is mandated in Iceland by law 50/1996, (the information act). The current Icelandic FOI law does not conform to CoE convention, and it does not match the standards set in the Aarhus convention for environmental information.[1]

An updated information act was proposed at Alþingi in 2011, however, due to end of term in late September 2011, the bill did not complete the third reading in parliament and was therefore dropped. It has since twice been reintroduced with many of the changes merged in and multiple improvements made.

IMMI submitted an 8 page report and a 84 page change comparison of the two bills to the constitutional and regulatory committee of Alþingi in February 2012, criticizing the government's backpedaling against the changes that had previously been proposed in parliamentary committee. At the moment, the committee work is proceeding.

Cautious optimism suggests that the bill will be accepted during the 141st parliamentary session, as the government has highlighted it as a priority. If this is the case, the norm for access to information in Iceland will be altered from being a 'publish on request' regime to 'publish by default' regime.[2] Then, any documents which are not published can be at least listed along with information about why it has been held back and FOI requests can be made for those documents specifically. This change is the most important alteration of many.

In the meantime, the new proposed constitution of Iceland has guaranteed a substantial improvement of information rights.[3]

[1] The Aarhus convention was ratified by law 131/2011.

[2] meaning that instead of FOI requests having to be made for each document individually in order to obtain a private copy for dissemination, which is a slow and complicated process, the rule will become that government publishes all documents publicly by default, for instance in an online database.

[3] http://www.stjornlagarad.is/english/ Articile 15 (English PDF available from the website)

Network Neutrality

Network neutrality is a very broad concept, but generally refers to the idea that each node operating on the network should be considered equal to all others in terms of access. Numerous governments and corporations have instantiated various forms of censorship and containerization#. Due to technical limitations of the IPv4 space, almost every end-user of the Internet can be considered in an aberration of the end-to-end principle often from NAT (Network Address Translation), this makes their nodes second class citizens of the Internet. There is a lot to be done in terms of network neutrality.

This is going to be a topic for many years, but for now IMMI has decided to take the first steps. Article 14 of the proposed constitution creates an obligation for the government to protect the Internet, with the same constraints as those on free speech in general. Although those limitations should definitely be questioned, this must be considered a substantial victory, as no country currently even mentions the Internet in its constitution, let alone defends it:

> Government shall guarantee conditions that are conducive to open and informed public discussion. Access to the Internet and information technology shall not be curtailed except by a decision of a court of law and on the same substantive conditions that apply to restrictions on the freedom of expression.

Communications Protection and Communications Data Retention

In the interests of protecting privacy and source confidentiality, protection of communications is a vital ingredient to any coherent information regulation strategy.

The protection of communications is a wide project that can be roughly split into two tasks. On the one hand, removing existing threats to communications protection from law, and on the other hand establishing new protections for communications.

In January 2012, as Alþingi was debating the adoption of the European Union's Data Retention Directive, IMMI produced a report outlining the dangers of blanket data retention. In committee, IMMI's views got the support of the Privacy Directorate, and this led to the parliamentary committee requesting that the directive be postponed indefinitely and that the foreign minister inform the European Union that Iceland would not be implementing the directive.

This however was not enough, as Iceland has in law a data retention clause (paragraph 3, article 42, of the telecommunications act, 81/2003, amended in 2005), which predates the EU's Data Retention Directive by a year. IMMI has argued against this clause, both in newspapers and in opinions to parliament, and has drafted a bill for the removal of the act.

More recently, IMMI was asked to submit proposals for improvement of certain articles of the telecommunications act being added to introduce a Computer Emergency Response Team (CERT) in Icelandic law, so as to better balance against privacy concerns. In these proposals, IMMI included the following proposal:

> Paragraph 3 of article 42, requiring the retention of telecommunication data, is dropped.
>
> Appended to article 42 is a new paragraph: Parties other than the sender and the receiver of electronic packet-switched communications are forbidden to inspect or electronically process the payload of the packets. Headers and metadata of packet-switched communications shall only be stored for the period needed to resolve the routing of the communications and security measures as per article 47. a.

This would effectively remove the data retention provisions from law, if adopted, and simultaneously improve the communications protection by making it a criminal offense to intercept and inspect communications, by methods such as Deep Packet Inspection. This exact wording was not adopted, but the intent of the second paragraph was included in the adopted law. The elimination of communications data retention has not yet happened.

In addition to this development, the proposed constitution of Iceland contains a clause in article 11 expressly forbidding the search of communications, except with a valid court order.[1]

[1] http://www.stjornlagarad.is/english/ Articile 11

Intermediary Liability Limitations

The original idea for limited liability for telecommunications intermediaries comes from the development of the Communications Decency Act in the United States around 1996. Since then, the European Union has adopted the e-Commerce Directive, which implements similar limitations. The directive is implemented in Iceland as the electronic commerce and other electronic services act (30/2002), and has equivalent measures.

Immediately on exploring the intermediary liability limitations (ILLs) in the Icelandic law, a striking flaw presents itself in the form of "general court orders". This phrasing is very vague and more importantly lends itself to being understood that district sheriffs, who in Iceland have injunctive powers, can issue takedown orders. IMMI has an interest in tightening this language, and intends to make proposals to do so in the coming months.

More importantly though, ILLs have been under attack globally in recent years. A great many changes in strategies relating to intellectual monopoly enforcement, protection of official secrets and political attempts at opening doors for corruption have revolved around eroding ILLs. In order to counteract this trend, IMMI has partnered with several organizations to explore what can be done to define a legal and technical defense of both Internet endpoints and intermediaries that can better withstand political attempts at erosion. This work is in the final stages, with results to be published in early October 2012.

Libel Tourism Protection

Libel tourism is the act of a company or individual choosing to pursue lawsuits against individuals or companies in a country with a low threshold for libel lawsuits. Legal extortion schemes have been perpetuated with companies being tried in countries such as England and Wales even if the defendant resides elsewhere in the world. This is a form of forum shopping. Implementing laws that prevent or diminish the effects of libel tourism in Iceland will protect Icelandic citizens and residents from this kind of forum shopping. It's fairly important that people can predict with some certainty where, if anywhere, they will be taken to court. This also applies to companies, who base a lot of their operational security on knowing the legal environment. In this way, ending libel tourism will encourage foreign investment and provide financial security for companies operating here already.

For now, Iceland has a mechanism. As a signatory of the Lugano treaty, Icelandic courts can decide not to uphold foreign court verdicts which go against the rule of law in Iceland. This means that a libel verdict from a foreign country can be challenged in an Icelandic court on the basis of article 34 of the Lugano treaty if it comes from a country with a substantially different burden of proof for libel than Iceland does. This has not been tested, but is currently our best bet.

In the meantime, British libel reform efforts are going well, and coupled with a well written libel law in Iceland, may be sufficient to put an end to libel tourism - at least in Iceland. When that is finished, the bigger issue of International Forum Shopping remains.

Libel Reform and Publishing Liability Limitations

The media law from 2011 introduced new rules regarding media liability. However, since its adoption, a number of court cases have been heard in Reykjavík which cast a shadow on the reform and point at a deeper structural fault in the current libel regime.

Although media liability is defined in the print law and superseded by the media law, the terms of libel itself are defined in chapter XXV of the criminal act, which treats violations of privacy and libel as equal criminal offenses. Under the criminal act, it is illegal to make truthful accusations, to offend somebody publicly or privately, or to make unfavorable comments about deceased persons. As these are criminal offenses, they have assigned imprisonment penalties from 1 to 4 years, as well as fines, although imprisonment is rarely used in practice.

The global trend in libel law is to move it away from criminal sanctions and into tort law, making it a civil offense, punishable only by fines. Alongside this, the scope of libel is to be narrowed, making the truth a valid defense and ensuring that people cannot be brought to charge for making value judgements against another's character. It should be legal to call a person a jerk, although it is questionable whether you can call somebody a murderous jerk without backing it up with evidence.

IMMI has completed the basic research needed to implement these changes and drafted a bill which aim to alleviate at least most of the existing concerns. Due to parliamentary scheduling rules, it cannot be introduced until the autumn of 2012.

Whistleblower Protection

A whistleblower is a person that tries to disclose or report information on situations affecting the public that may evidence of criminal activity. Protection for individuals reporting institutionalized corruption is paramount. They may be providing relevant information to the public record, such as data or testimony about relevant matters like public health, passed incidents, crime, government biases, democracy undermining practices, violations of constitutional rights, corruption and bribery.

Threats to whistleblowers come from corporate interests, governmental interests, criminal activities, biases inherent in legal and judicial officials and systems. Whistleblower protections must include a right to anonymity, physical, financial and social security.

As the threat models, institutional settings and personal complexities of whistleblowing vary widely, this is perhaps the most complicated of IMMI's tasks. While a lot of development work has been put into this issue already, we feel that the adequate protection of whistleblowers cannot be completed without deep investigation.

As one core issue, the idea of corporate personhood must be challenged. Disregarding other arguments for doing so, it is very important that it not be decided that companies and other corporate vehicles have a right to privacy, as this would pit whistleblower activities up against privacy and data protection law, the sanctity of which is of equal importance. It's a fight nobody should have to fight. That said, there has been no such ruling in Iceland and it is not foreseeable that that will change; it's merely one issue of many that must be monitored and pro-actively taken action on.[1]

[1] For more detail see:: http://immi.is/Press_Release:_IMMI_Status_Update,_April_2012

Prior Restraint Limitations

Prior restraint is banned under article 73 of the Icelandic constitution. A slightly stronger implementation of prior restraint limitations are introduced in the new constitution, which is pending ratification.

Outside of constitutional guarantees, IMMI also has an interest in protecting against abuse of injunctions by sheriffs, who still have injunctive authorities as a holdover from their now abolished tribunal role. This fits in with the discussion of Intermediary Liability Limitations stated above, and IMMI expects to be able to address these two concerns jointly.

Virtual Limited Liability Companies

Icelandic corporate law is currently somewhat hostile to foreign ownership from outside the European Economic Area (EEA). The idea of Virtual Limited Liability Companies is to allow for virtually defined corporate entities, whereby the ownership is somewhat ephemeral, as long as the owners adhere to certain Icelandic transparency requirements. In that way, a virtually operated commpany would have tax obligations and operational safe harbor rights in Iceland like any other company, but gets to operate virtually in exchange for some strict guarantees of transparency and such.

This issue has more to do with creating a pleasant investment environment than explicitly improving the information regime in Iceland. For that reason, it has been relegated to the set of the last things we aim to accomplish in this set, and is therefore on hiatus for now.

Selected Bibliography

- Orkustefna fyrir Ísland; Stýrihópur um mótun heildstæðrar orkustefnu; http://www.nea.is/media/gagnasofn/Orkustefna-fyrir-Island.pdf

- Iceland. What a Great Place to Put a Data Center; Verne Global / Martin Hannigan; http://www.uknof.org.uk/uknof12/Hanningan-Undersea.pdf

- Orkuspá fyrir Ísland 2010-2050; Orkustofnun; http://www.os.is/gogn/Skyrslur/OS-2010/OS-2010-07.pdf

- Benchmarking Study on Iceland as a Location for Data Centre Activity; Invest in Iceland Agency; http://www.invest.is/resources/files/invest.is/BDC%20Report.pdf

- Mikil arðsemi af raforkusölu til stóriðju; Vísir; http://www.visir.is/mikil-ardsemi-af-raforkusolu-til-storidju/article/2011712209851

- Policy Mix for Innovation in Iceland; OECD; http://www.oecd.org/dataoecd/15/62/36648108.pdf

Appendix A: Model Details

The details of the rubric questions used are presented here, split into the same three sections as the rest of the evaluation. For detailed discussion of each issue, see the relevant section above.

Energy

Energy Sources

Source Renewability:

How prevalent are renewable energy sources in current electrical production?

1. Less than 3% of all energy production based on renewable energy sources.
2. Between 4 and 40% of all energy production based on renewable energy sources.
3. Between 40 and 60% of all energy production based on renewable energy sources.
4. Between 60 and 97% of all energy production based on renewable energy sources.
5. More than 97% of all energy production based on renewable energy sources.

Source Scalability:

How much can current electrical production be increased without the construction of new (not currently planned) power plants?

1. By less than 5% of current average power use.
2. By less than 25% of current average power use.
3. By less than 50% of current average power use.
4. By more than 75% of current average power use
5. By more than 100% of current average power use.

Supply Price:

What is the annual average price per kiloWatt hour for a commercial customer using less than 2 GWh/year, including generation and distribution?

1. > €0.20/kWh
2. > €0.14/kWh
3. <= €0.14/kWh
4. < €0.09/kWh
5. < €0.07/kWh

Generation

Generation Redundancy:

How much auxiliary power is available on the electrical grid at any given time, as a percentage of the total energy production?

1. <1%
2. >1%
3. >3%
4. >5%
5. >7%

Generation Reliability:

How frequent are outages at power plants?

1. Frequent
2. Infrequent
3. Uncommon
4. Rare
5. Very rare

Grid

Grid Redundancy:

How well connected is the power grid, with respect to the ability to compensate if partial grid failure occurs?

1. Sparsely connected (E ~ N)
2. Redundancy only on some larger links, weak secondary links (readily separable graph)
3. Most major links have redundant connections, only a small number of weak interties
4. No single points of failure with sufficient capacity on secondary links; generally a single merged graph
5. Fully connected (E ~ (N*N-1)/2)

Grid Reliability:

How frequent are grid failures?

1. Frequent
2. Infrequent
3. Uncommon
4. Rare
5. Very rare

Environment

Average Temperature:

What is the average temperature in the country?

1. >20°C
2. <20°C
3. <15°C
4. <10°C
5. <5°C

Cold Water Availability:

How available is clean cold water (not necessarily potable, but at least sufficient for cooling purposes)?

1. <1.000 m^3
2. <10.000m^3
3. >20.000 m^3
4. >50.000 m^3
5. >200.000 m^3

Average Humidity:

What is the average humidity in the country?

1. >90%
2. >75%
3. <60%
4. <45%

5. <30%

Power Usage Efficiency:

What is a typical PUE (Power Usage Effectiveness) of a data center in the region?

1. <12
2. <8
3. <4
4. <2
5. <1.5

Freedom from Natural Hazards:

How frequently and how severely do natural hazards disrupt power, transport, and communications in the country?

1. Frequently/Significantly
2. Infrquently/Moderately
3. Uncommonly/Slightly
4. Rarely/Minorly
5. Very rarely/Very minorly

Connectivity

Domestic Connectivity

Redundancy:

How much infrastructural elasticity is there in the domestic telecommunications network?

1. Many single points of failure for all connectivity. Few or no redundant links. Many or most links are legacy copper.
2. Many single points of failure but at least moderate protection. Mix of copper and fiber networking plant, with some link redundancy.
3. Some single points of failure, at least moderately well protected. Most links are fiber and many are redundant, but the failure of some single fiber strands can significantly reduce effective deployed capacity.
4. Few or no single points of failure; any such are well-protected. Most connectivity is fiber and important connections have redundant links, frequently in bidirectional rings. Few single fiber breaks will significantly reduce effective deployed capacity.
5. No single points of failure at any non-endpoint in the network. All important links are fiber and have multiple redundant geographically diverse cables in bidirectional ring configurations capable of independently serving full deployed capacity.

Reliability:

How reliably does telecommunications data make it to its intended destination?

1. <99% of the time.
2. <99.9% of the time.
3. <99.99% of the time.
4. <99.999% of the time.
5. >99.999% of the time.

Scalability:

How much can the current infrastructure scale up in demand without more infrastructure having to be added?

1. <25%
2. >25%
3. >50%
4. >100%
5. >200%

Throughput:

What is the available additional throughput of the current infrastructure?

1. <100Gbps
2. >100Gbps
3. >1Tbps
4. >10Tbps
5. >100Tbps

Latency:

How much natural latency is there in the domestic network?

1. >30ms
2. <30ms
3. <15ms
4. <7.5ms
5. <5ms

Expansion:

How great are current plans for expansion of the infrastructure?

1. <25%
2. >25%
3. >50%
4. >100%
5. >200%

CERT Responsiveness:

What is the level of preparedness and responsiveness of the state's CERT team, if it has one?

1. No CERT team available; little or no organized response.
2. Basic CERT team in place with relatively little operational experience, few organizational ties, and little or no capacity for handling multiple simultaneous incidents.
3. Experienced CERT with some organizational integration and the ability to handle complex or multiple incidents.
4. Very experienced CERT team with good integration with most hosting providers and enterprises. Proven capability to handle multiple complex simultaneous incidents.
5. Immediate response to all issues from a highly trained CERT team seamlessly integrated with internal security teams at all hosting providers and enterprises with significant online presences.

DDoS Outage Frequency:

How frequently are there temporary outages in parts of the domestic system as a result of DDoS attacks?

1. >Daily
2. >Weekly
3. >Monthly
4. >Yearly
5. <Yearly

Targeted Attack Incidence:

How frequently is the state's network infrastructure subject to significant targeted attacks from abroad?

1. >Daily
2. >Weekly
3. >Monthly
4. >Yearly
5. <Yearly

Central/Western Europe

Redundancy:

How much infrastructural elasticity is there in the telecommunications network to the area in question?

1. Many single points of failure for all connectivity. Few or no redundant links.
2. Many single points of failure but at least moderate protection against failure.
3. Some single points of failure, at least moderately well protected. Many links are redundant, but the failure of some single fiber strands can significantly reduce effective deployed capacity.
4. Few or no single points of failure; any such are well-protected. Important connections have redundant links. Few single fiber breaks will significantly reduce effective deployed capacity.
5. No single points of failure. All important links have multiple redundant geographically diverse cables in capable of independently serving full deployed capacity.

Reliability:

How reliably does telecommunications data make it to its intended destination?

1. <99% of the time.
2. <99.9% of the time.
3. <99.99% of the time.
4. <99.999% of the time.
5. >99.999% of the time.

Scalability:

How much can the current infrastructure scale up in demand without more infrastructure having to be added?

1. <20%
2. <30%
3. >50%
4. >100%
5. >200%

Throughput:
What is the available additional throughput of the current infrastructure?

1. <1Gbps
2. >1Gbps
3. >10Gps
4. >100Gbps
5. >1Tbps

Latency:
How much natural latency is there in the network to the region in question?

1. >100ms
2. <100ms
3. <66ms
4. <33ms
5. <16ms

Expansion:
How great are current plans for expansion of the infrastructure?

1. <20%
2. <30%
3. <50%
4. >100%
5. >200%

North America

See Central/Western Europe.

Eastern Europe/Russia

See Central/Western Europe.

Middle East and North Africa (MENA)

See Central/Western Europe.

East/South-East Asia

See Central/Western Europe.

Jurisdiction

State Security Burdens

Surveillance Burden:

How strong are state imposed surveillance requirements?

1. The state imposes full electronic surveillance of all telecommunications.
2. The state performs pervasive monitoring of selected portions of telecommunications networks, either targeted at individuals or groups, or on certain links, such as border crossings.
3. The state requires ISPs to submit traffic logs to government agencies for inspection either regularly or upon request.
4. The state requires telecommunications data retention, but otherwise does not require or perform any surveillance.
5. The state does not perform or require any electronic surveillance.

Censorship Burden:

Does the state mandate censorship, or are there protections against state mandated censorship?

1. The state runs extensive censorship infrastructure directly or through ISPs.
2. The state often takes down, blocks or otherwise censors particular keywords, websites or other communications traffic, with or without court orders.
3. The state often takes down, blocks or otherwise censors specific websites after getting a specific court order.
4. The state does not perform any censorship.
5. The laws of the state explicitly forbid censorship.

Data Retention Burden:

Does the state require telecommunications data retention?

1. Yes, and there is frequent illegitimate access to the data
2. Yes, for more than 6 months
3. Yes, for 6 months
4. No
5. The state forbids retention of telecommunications data for longer than necessary for billing purposes

Key Escrow Burden:

What kind of encryption key escrowing, if any, does the state require?

1. The state requires escrow of all encryption keys.
2. The state requires escrow of all keys of a certain size, or has weak conditions for the requirement of key escrowing.
3. The state does not require escrow of keys in general, but can request key escrow at any time.
4. The state does not require escrow of keys in general, but can require keys to be handed over as part of criminal investigations.
5. The state does not require any escrowing of keys.

Network Militarization Burden:

Is the state engaged in an electronic military buildup?

1. The state has engaged in hostile actions through the Internet.
2. The state has actively been developing and testing Internet-based weapons.
3. The state is active in both offensive and defensive electronicmilitary buildup.
4. The state is engaged in defensive electronic military buildup.
5. The state is not engaged in electronic military buildup of any kind.

Competitive Landscape

Software Patent Burden:

What kind of software patent regime does the state have?

1. Software patents exist in law and are enforced in practice, both on local developers, and imported software.
2. Software patents exist in law, and are enforced in practice on local developers.
3. Software patents exist in law, but are not enforced.
4. There is no legal basis for software patents, but software patents are granted in practice regardless through alternative mechanisms.
5. There is no legal basis for software patents.

Anti-Monopoly Protection:

How strong are the state's anti-monopoly protections?

1. The state actively endorses numerous monopolies.
2. The state supports some monopolies in relevant industries, such as telecommunications, and is inactive in breaking others up.
3. The state weakly supports some monopolies and has anti-monopoly statutes in place for some industries, but they are rarely used.
4. The state does not support any monopolies directly and has anti-monopoly statues in place, which are used occasionally.
5. The state is very active in disassembling monopolies or reprimanding companies for monopolistic actions.

Libel Tourism Protection:

Does the state have protections against cross-jurisdictional abuse of weak libel laws in other states?

1. No, and the state is a party to a treaty or International directive which precludes such protections being adopted.
2. No.
3. No, but courts have been known to require separate hearings prior to enforcement.
4. Some. Functionally equivalent to article 34 of the Lugano Treaty.
5. Yes.

Carrier Liability Limitation:

Are carriers protected from liability created by their users' activities?

1. Carriers are fully liable for activities taking place on their networks.
2. Carriers are expected to monitor for certain types of behavior, and can be found liable if derelict in this obligation.
3. Weak liability limitations exist, but in practice carriers are often threatened directly because of user activities.
4. Yes, a intermediary liability limitations regime is in place, at least eliminating any obligation to monitor.
5. Yes, a fully functioning intermediary liability limitations regime is in place.

Intermediary Liability Limitation:

Are telecommunications intermediaries protected from liability created by their users' activities?

1. Telecommunications intermediaries are fully liable for activities taking place on or enabled by their systems..
2. Telecommunications intermediaries are expected to monitor for certain types of user behaviour and can be found liable if derelict in this obligation.
3. Weak liability limitations exist, but in practice telecommunications intermediaries are often threatened directly because of user activities.
4. Yes, a intermediary liability limitations regime is in place, at least eliminating any obligation to monitor.
5. Yes, a fully functioning intermediary liability limitations regime is in place and includes non-carrier intermediaries.

Network Neutrality:

Does the state violate or protect network neutrality?

1. No. Network neutrality is grossly violated in the state.
2. No. Network neutrality is violated on at least one type of network.
3. No, but network neutrality violations are infrequent or nonexistent.
4. Yes, the state actively applies consumer protection or other statutes to reprimand network operators for neutrality infractions.
5. Yes, a law guarantees network neutrality.

Takedown Notice Regime Burden:

Does the state have an active notice- and takedown regime for copyright violations?

1. Takedown notices are used very aggresively, have no due process protection, notification, or appeal rights, and confer direct liability to a non-respondent intermediary.
2. Takedown notices are common and have no due process protection or notification process, confer direct liability to a non-respondent intermediary, but can be appealed.
3. Takedown notices are common, have no meaningful due process protection, and confer direct liability to a non-respondent intermediary, but do require notification and permit appeal.
4. Takedown notices are infrequent and require full notification of all parties, have a right to appeal and no confered liability for non-malicious noncompliance, but do not require a court order.
5. Takedown notices require a court order with full notification of all parties, right to appeal, a ban on any presumptive action, and no confered liability for non-malicious noncompliance.

Commercial Issues

Capital Restriction Burdens:

Are there any restrictions on the flow of capital?

1. Yes, capital controls are in place. All capital flows are subject to permission from central authority.
2. Capital flows are controlled beyond certain amounts and require active notification for all amounts.
3. Capital flows are controlled beyond certain amounts.
4. Capital flows are controlled internationally, but not within the geographic region (such as EU).
5. No capital controls are in place.

Currency Market Size:

Is the currency market (m2) sufficiently large to support large influxes of investment?

1. <10 billion EUR
2. <100 billion EUR
3. <1.000 billion EUR

4. <10.000 billion EUR
5. >10.000 billion EUR

VAT Burden:

How high are the top bracket VAT rates?

1. >25%
2. >20%
3. >15%
4. <=15%
5. 0%

Equipment Import Duty Burden:

What is the burden of import duties for equipment?

1. >100%
2. <100%
3. <50%
4. <15%
5. 0%

Service Provision VAT Burden:

How high is the VAT for service provision?

1. >25%
2. >20%
3. >15%
4. <=15%
5. 0%

Corporate Tax Rate Burden:

What is the corporate income tax rate?

1. >33%
2. <33%
3. <20%
4. <15%

5. <10%

Legal Friction

Incidence of Sanctions:

How frequently has the jurisdiction been a target of sanctions, in particular those covering the import of ICT hardware and software from major markets or the export of services?

1. All ICT exports to the country have been banned by most major producers and have been for a decade or more.
2. The export of some ICT products to the country has been regularly banned for significant periods of time.
3. Some export regulations for technologies, particularly "dual-use" technologies, have been in place on a regular basis from some major producers.
4. Few if any regulations have existed on technology exports to the country from any producer, possibly excepting dual-use technologies.
5. Never.

Legal Stability:

Is the jurisdiction's legal system stable enough to allow for long-term planning by enterprises?

1. Frequent radical changes have occurred in basic founding documents or the fundamental legal structure. Specific regulations are in constant flux, when defined.
2. Siginficant changes to basic legal structures have happened on a regular basis in recent history. Regulatory changes happen often and with little or no notice.
3. The basic legal structure of the country has changed significantly in the past 50 years. Regulatory changes happen frequently, sometimes with relatively little notice.
4. The fundamental legal structure of the country has evolved over the last century. Changes to the regulatory regime happen frequently, but with notice.
5. Few or no significant changes have occurred to the fundamental legal structure in the past century, which is well-defined and well-understood. Regulation changes slowly and with significant notice and explanation.

Strength of Rule of Law:

Does the rule of law have sufficient force in the jurisdiction to present a functional framework for business?

1. There is no effective recourse to the rule of law for most issues, including basic property disputes.
2. It is possible to invoke the rule of law for most issues but it is frequently ineffective; corruption is rampant.
3. The rule of law is generally in effect, although significant corruption exists and due process can be slow at best.
4. The rule of law is effective in all areas, but may be slow; some corruption exists.
5. The rule of law is efficient and complete.

EU Directive Compatibility:

How compatible is the jurisdiction with EU acquis communitaire?

1. The jurisdiction is incompatible with EU law.
2. The jurisdiction has some laws which are compatible with EU law.
3. The jurisdiction has implemented over 40% of EU law or equivalent law.
4. The jurisdiction has implemented over 60% of EU law or equivalent law.
5. The jurisdiction has implemented over 80% of EU law or equivalent law.

Human Resources

Availability of Qualified Workforce:

How many unemployed or underemployed qualified ICT professionals exist in the country?

1. <25k
2. >25k
3. >50k
4. >100k
5. >200k

Average Wage Burden:

What is the average wage burden for a qualified IT professional in the country?

1. >€175.000/year
2. >€125.000/year
3. >€75.000/year
4. >€50.000/year
5. <€50.000/year

Social Welfare Burden:

What is the average additional burden for social welfare for a professional employee, above and beyond wages?

1. >50%
2. >40%
3. >30%
4. >20%
5. <20%

Immigration Flexibility:

How easy is it for an enterprise to import key personnel temporarily or permanently?

1. Immigration is hindered by legal restrictions. Work visas require substantial vetting.
2. Immigration is subject to many restrictions. Work visas require minimal vetting and corporate sponsorship.
3. Immigration is open within the region, but work visas for people from outside the region are harder to get.
4. Immigration is open within the region. Work visas for people from outside the region are granted if requested by a company.
5. Immigration is open. It is easy to get work visas with very few restrictions.

Language Compatibility:

What percentage of the professional workforce speak one or more common business languages?

1. <1%
2. <5%
3. <25%
4. <50%
5. >50%

Locale is rapidly becoming one of the most important competitive differentiators in the provision of cloud-based information technology services. Broadly speaking, three categories of issues define a locale's fitness for hosting the cloud: energy, connectivity, and jurisdiction.

Energy is the largest cost center for most cloud hosts. Beyond price per kilowatt hour, hosting companies must consider redundant network availability, power grid resilience, environmental sustainability, climate, and equipment cooling requirements as core parts of their energy strategy.

Connectivity is clearly essential for hosts, and differentiating factors here include total installed bandwidth, current utilized bandwidth, hub redundancy, international uplink redundancy, round trip latency, traffic shaping and network neutrality.

Jurisdictional issues are an area of emerging concern and awareness for cloud hosts, where the landscape is shifting rapidly. Hosting companies are deeply affected by intermediary liability, hosting liability, state and corporate surveillance, state and corporate censorship, the accessibility of and cost of interacting with courts, corruption, and socioeconomic stability.

This report lays out a comparative model for these topics. Intending to serve as the basis for further analysis into the comparative qualities of different countries, throughout Europe and the world, the model considers roughly 80 variables, each of which is assigned a rubric-based score from 1-5. In order to demonstrate the utility of this model, Iceland's relative competitive advantages and drawbacks as a hosting locale are mapped out using it.