golden frog

# Peace, Prosperity & the Case for the Open Internet

A SHARED VISION AND CALL TO ACTION FOR THE NETIZENS OF THE WORLD

*by **Ron Yokubaitis**, Co-Founder and Co-CEO of Golden Frog*

## The Challenge to Freedom

No matter what age, or kingdom; no matter what social contract or court of law, there is perhaps one course of action that one can always count on—that man will always think he knows what's best for his neighbor.

Ruling one's neighbor is not always about control or slavery. Perhaps the worst kind of ruler is one governed by benevolence. When we seek to control information and experience in the name of protecting those who do not know best, we are simply the serpent protecting the Tree of Knowledge from those we deem to be naked and ignorant. A society that dictates what we have the right to read and learn and seek and explore cannot be prosperous. Only a free and informed people can achieve prosperity and peace, and protect their liberties.

**LIKE THE VAST OCEANS OF THE WORLD, THE INTERNET CONNECTS US**

Throughout history, mankind has been an explorer—seeking to rise above internal and external limitations and challenge the oceans, mountains and mysteries of the world. We are still explorers.

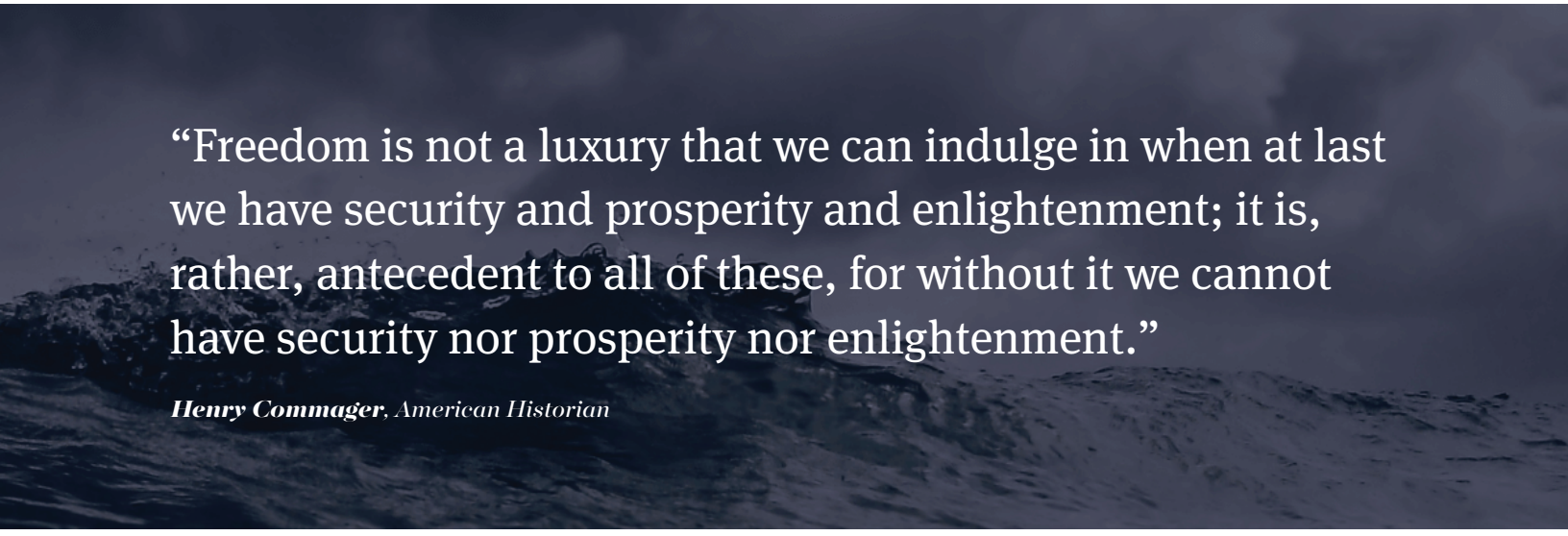
But today we can explore our world without leaving our homes. With the power of global networks, we are connected—person to person, machine to machine,

and data to data. The world is literally at our fingertips. Like the vast oceans of the world, the Internet connects us.

But there are still those who believe they know what's best for their neighbor. There are those who believe that censorship and control are necessary. They paternalistically claim they are trying to protect us from ourselves or others, but in reality they are trying to protect themselves from our own exercise of liberty. As a result, we are faced with a global challenge to freedom. Despite the Internet's pervasive role in commerce, communication and our communities, millions of people continue to be restricted by benevolent governments and corporations.

Not only does Internet access continue to be restricted, but these restrictions are increasing in many parts of the world. Freedom House, a watchdog organization dedicated to the expansion of freedom, reported in their Freedom on the Net 2014 report that worldwide Internet freedom was on the decline for the fourth year in a row. The reasons for this decline include an increase of surveillance, repressive laws, regulations on media usage and cyber attacks. 46 of the 65 countries examined were ranked as having an Internet experience that was only “partly free” or “not free.” Furthermore, 19 of the countries “passed new legislation that increased surveillance or restricted user anonymity.” [1]

1 Freedom House, Freedom on the Net 2014. Copyright © 2014 Freedom House, available at https://freedomhouse.org/sites/default/files/resources/FOTN%202014%20Summary%20of%20Findings.pdf




Many technology service providers are asked by governments to ban access or availability of certain content. Large Internet service providers often prevent users from accessing content or websites that their governments declared illegal or undesirable, while leaving the content available for users in other countries in which certain prohibitions are not in effect.

Google's Transparency Report shows that 63 countries asked it to restrict access to certain content in the first six months of 2014. And in 2013, Google was asked to remove over 39,000 items from its search results and other sites. In the United States, legislators want more technology firms to do the same. [2]

2 Google, Google Transparency Report. Copyright © 2015 Google, available at http://www.google.com/transparencyreport/removals/government

A congressional subcommittee approved revisions to the Global Online Freedom Act in March 2012. Based on these revisions, technology companies that operate in a selected group of restrictive countries would have to publish annual reports revealing how they deal with human rights issues. This would not be required of companies that join associations that provide similar oversight such as the Global Network Initiative, which protects and advances the "freedom of expression and privacy in information and communications technologies."

In 2012, the Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) failed to pass because of public outcry and protests. The bills attempted to protect music artists and corporations from copyright infringement by limiting Americans' freedom on the Internet through the exercise of regulatory control over much of the online space. More than three years after SOPA's and PIPA's rejections, there are other lesser-known bills pending in Congress that would limit Internet users' freedom and invade their privacy by allowing certain entities to access personal data. The Cyber Intelligence Sharing and Protection Act (CISPA) would allow warrantless searches and sharing of personal data among and between private companies and the government. The Cybersecurity Information Sharing Act (CISA) of 2015 was introduced in Senate in March 2015. This bill allows companies to monitor user information and encourages them to share it with the government. Despite strong public opposition, these types of bills continue to be proposed.

**CISPA WOULD ALLOW WARRANTLESS SEARCHES AND SHARING OF PERSONAL DATA**

Governments are not the only restrictive bodies. American companies can also restrict content. Many websites do so to protect individuals from obscene or slanderous material or do their best to avoid potentially offending visitors or contributors. The majority of users support website policies that prohibit hate speech or obscene content, despite the fact that much of the prohibited speech is protected under First Amendment principles. Community groups also try to limit what can be shown or displayed.

Access to pornography on the Internet remains a contentious issue. Though seen as obscene and offensive to some, pornography is not prohibited in the United States. Under the law, consenting adult participants can produce, distribute and purchase these materials. The quality and appropriateness of online content is subjective and should not be restricted solely because individuals or groups express opposition or discomfort. Adults should have the

right to access what they want and share what they want online except under circumstances that exploit or do harm to individuals, particularly children, who cannot adequately defend or protect themselves.

Kevin Bankston, Director, Open Technology Institute, said that fervent moderation can have "absurd and censorious" results. In September 2012, Facebook removed a cartoon of a bare-chested Eve in the Garden of Eden that was published by The New Yorker due to Facebook's policy to remove content that is sexually loaded. In 2015 Facebook exercised similar censorship when it removed a photo of a 19th century painting, and again when it censored images of the prophet Muhammad in Turkey.

Some companies protect the interests of their partners as was the case with Twitter in 2012. Twitter suspended the account of a journalist who criticized NBC, a business partner of Twitter's, for inadequate coverage of the London Olympics and then published the email address of an NBC manager. Initially, Twitter said that publishing a personal email address was a violation of their privacy policy. Twitter's general counsel later informed the public that suspending the account was a mistake and they do not proactively monitor or remove content on behalf of others.

**FERVENT MODERATION CAN HAVE ABSURD AND CENSORIOUS RESULTS**

Although protecting the interest of one of its partners was not intentional, Twitter demonstrated that it is able to and will restrict content. YouTube is another provider that is not immune to automated flagging. The site's probing system temporarily blocked a video of Michelle Obama speaking at the Democratic National Convention in September 2012 and had also blocked NASA footage of the Curiosity rover landing on Mars in August 2012.

As lawmakers, service providers and freedom protection groups combat governments and policies that suppress freedom on the Internet, it is clear that restrictive Internet policies will continue to be an obstacle for those seeking and advocating for an open Internet.

## Encryption is the Second Amendment of the Internet

Keeping information private and accessible only to those given direct access has become an increasing concern as the amount of content being stored online continues to increase exponentially. Online "cloud" storage solutions are now mainstream, and many are turning to encryption as a way to protect their

private data. This has led many governments to question whether they should control citizens' right to encrypt data or communications and if governments should have the right to decrypt private information.

In 2015 the United States FBI and Justice Department pushed for legislation that would require a “backdoor” into encrypted communications. This backdoor was advocated for in the name of security, but it opens up online communications to vulnerabilities and threatens innovation and the technology community at large.

The extension to the Foreign Intelligence Surveillance Act (FISA) to 2017 allows the U.S. government to conduct warrantless searches of Internet users. Governments have argued that they need to search the Internet and decrypt data in order to properly identify and apprehend thieves and terrorists. However, this act may undermine due process by making all online data subject to search and seizure without notifying the owner and without probable cause.

**ENCRYPTION IS A NECESSARY TOOL FOR DATA SECURITY & TECHNOLOGICAL INNOVATION**

Companies have been more supportive of encryption than government bodies. The right of encryption was bolstered by HTTPS, a secure protocol option for Web surfers, that is becoming more widely used in the last few years by companies that want to provide users a safe connection for their Web visitors. The Electronic Frontier Foundation (EFF) and The Tor Project collaborated on "HTTPS Everywhere," an extension to browsers Mozilla Firefox and Google Chrome that encrypts users' communications with many websites. Many Silicon Valley and technology companies banded together in protest of the FBI’s 2015 request for encryption backdoors, defending encryption as a necessary tool for data security and technological innovation.

Encryption is analogous to the Second Amendment. It is, quite simply, the right to defend oneself. And like those who defend the constitutional right to bear arms, we must remain ever vigilant. Legislation like FISA inhibits our freedom and violates our privacy. From text messages to browsing history to online downloads, we have a right to communicate and view information privately.

A free and open Internet requires that tools be made available to help consumers protect their private data. The right to bear encryption keys is a necessary policy if we are to defend the right to privacy.

# The False Promise of Net Neutrality

In 2005, the Federal Communications Commission set out to keep the Internet open to consumers by establishing the Open Internet Order. This set of regulations prevents network providers from restricting content their users access and limiting the services they use. The four principles of the order are:

1. **Consumers deserve access to the lawful Internet content of their choice.**
2. **Consumers should be allowed to run applications and use services of their choice.**
3. **Consumers should be able to connect to their choice of legal devices.**
4. **Consumers deserve to choose their network providers' application, service providers and content providers.**

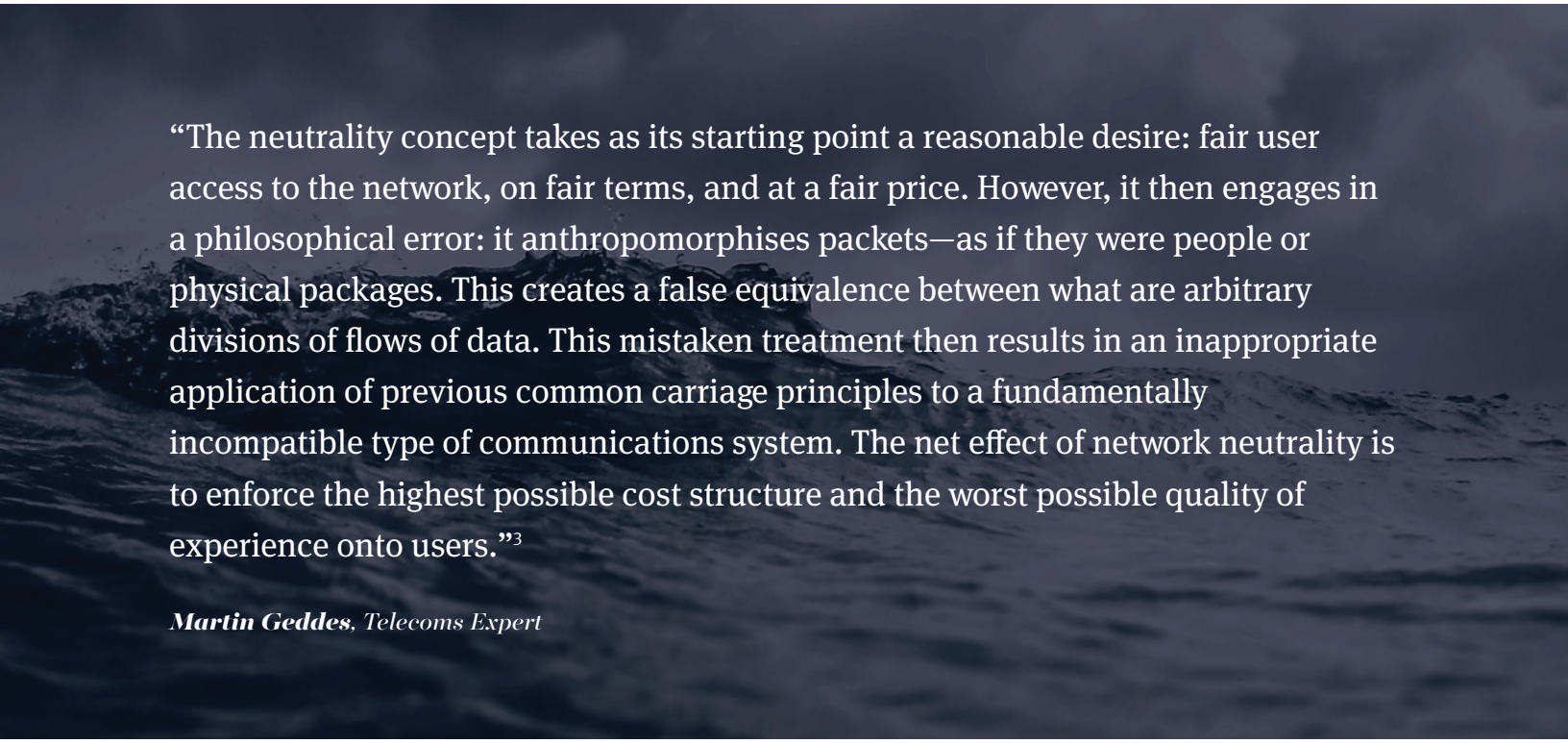
The Open Internet Order led to the establishment of the Internet neutrality concept, which argues that network providers cannot inhibit the information that is transmitted through their networks and all users must be granted equal access. The FCC later created two tiers of Internet access: fixed-line providers and wireless providers. They both follow rules about transparency, content blocking and unreasonable discrimination.

The discussion over "Open Internet" began with good intentions and if properly implemented could have been a positive step to continuing Internet users' freedom. The problem is that while the FCC was trying to protect consumers and promote an open Internet, the net neutrality approach they took was misguided, and consigned to inevitable failure. The "problem" did not reside with those who provide "Internet." This service sector could quite easily be fully competitive, if only the underlying transmission components remain available on a common carrier basis, and thus reasonable and nondiscriminatory terms. If this were to occur, then any "Internet" provider that failed to act in a manner consistent with consumer expectations would quickly be faced with alternative providers that provided what users really want. As it stands, however, the "last mile" transmission is available only to the telephone and cable companies, and only they can provide "Internet." They therefore can now monopolize (or duopolize) both the transmission and the "Internet access."

**THE OPEN INTERNET ORDER IS A STEP IN THE RIGHT DIRECTION, BUT THERE'S STILL MUCH TO ADDRESS**

The second problem is that "net neutrality" concepts were based on premises that cannot be extended to "the Internet."

Martin Geddes explains the basic problem:



> “The neutrality concept takes as its starting point a reasonable desire: fair user access to the network, on fair terms, and at a fair price. However, it then engages in a philosophical error: it anthropomorphises packets—as if they were people or physical packages. This creates a false equivalence between what are arbitrary divisions of flows of data. This mistaken treatment then results in an inappropriate application of previous common carriage principles to a fundamentally incompatible type of communications system. The net effect of network neutrality is to enforce the highest possible cost structure and the worst possible quality of experience onto users.”[3]
>
> ***Martin Geddes**, Telecoms Expert*

The FCC created a false sense of protection and hope for consumers. The agency enforced policies to protect consumer rights that may not have been in jeopardy initially. Net neutrality was supposed to give consumers more choice, control and access. By imposing these regulations, however, the FCC undoubtedly prevented online and network services from being created and benefiting consumers.

As a consequence, net neutrality possibly slowed innovation among technology companies. This regulation did not allow "Internet access" providers to charge other providers to use or share their services. Service provider partnerships could have spurred further innovation and created new business models for revenue growth and economic prosperity.

Over the years, the Open Internet Order's regulations have softened, and restrictions on companies have loosened. But, while service providers continue to challenge the regulations and propose new legislation, this new legislation is just as harmful.

3 Martin Geddes, Network neutrality: nasty or nice?, Copyright © 2013 Martin Geddes Consulting Ltd, available at http://us1.campaign-archive1.com/?u=f105fd56904428bca9da44a828&id=eef3b03292.

## PROVIDERS STILL HAVE TOO MUCH CONTROL, AND USERS ARE VULNERABLE

There's a reason that service providers fight to achieve a dominant position—monopoly or duopoly. They can create merely toll roads on the data freeway that, rather than charging by the mile (or gigabyte), attempt to capture rents based on the value of the content rather than the cost of providing the service. Despite the fact that every megabyte or gigabyte costs the same, providers are seeking to charge for content and the value they think they can derive.

It is analogous to converting a "freeway" paid by taxpayers into a private toll way. Just like the monopoly telephone companies whose infrastructure was paid by ratepayers for 100 years, the infrastructure is still being "maintained" by user fees. What was previously open to all applications is now closed to only those applications approved by the access providers—who control the underlying infrastructure.

In March of 2015 the United States FCC released its Open Internet Order, which addressed some of these issues. While regulation isn't favorable, in the absence of competition it is necessary to have light regulation. Market competition does not exist within the duopolized ISP market, so the Open Internet Order puts into place necessary, but light, regulations. It's a step in the right direction, but there is still much that has not been addressed. Providers still have too much control, and Internet users are vulnerable to all sorts of barriers to an Open Internet including "fast lanes" and encryption-blocking technologies. An Open Internet will only exist with a truly competitive market that allows users to choose an ISP that respects their privacy while also providing excellent service.

# Impacts on Privacy

ISPs and telecom companies have the capability to store everything that passes to and from your computer over the Internet, and with the implicit permission and support of the U.S. government, can perform surveillance, monitoring and store your private communications. The deafness of Congress, the FCC and the FTC to this unwarranted surveillance was a catalyst for Golden Frog to get involved and create encryption and private storage solutions for the consumer. The Usenet went encrypted six years ago (Giganews.com). Now the Web is spawning pay encryption service providers to protect the retail Internet user. The price of freedom on the Web unfortunately has a high price.

**FREEDOM ONLINE UNFORTUNATELY HAS A HIGH PRICE**

Privacy is not the same as anonymity. With privacy you can choose your identity. If you want to be a dog you can pretend to be a dog, but they [ISPs and telecom companies] will know everything you say while pretending to be a dog.

And when they decide it is time to chase the dog, they will be able to follow your scent via the trail left behind by your communications.

Is it our role as a society to govern what our neighbor can know or learn or see? Does our own benevolence betray us?

# We Must Build Tools to Protect People

Regulations and laws cannot stop technology from empowering people. As government regulations on the Internet and privacy fluctuate, the best thing Internet proponents can do is continue to create solutions and promote the peaceful and free use of the Internet.

At Golden Frog we are fighting for a free and open Internet, and for fair access to the infrastructure that could support competitive Internet access. We believe the best hope for this is to allow technological innovation to create tools and resources for autonomous people to explore the ocean of ideas, communicate, search, find and exercise their right to free expression and commerce. Golden Frog was created to develop services that give people the ability to defend and protect themselves online.

**AT GOLDEN FROG WE ARE FIGHTING FOR A FREE AND OPEN INTERNET**

We build the applications and tools that enable us to advance freedom and to keep the Internet open. Created and supported by an experienced team, VyprVPN and Cyphr are two innovative solutions that ensure that Internet users can securely and safely access websites and files while protecting their personal information and privacy. Future services will do the same.

These solutions allow users to stay connected and maintain relationships around the world regardless of location. Compatible across operating systems, the tools can be enjoyed by most Internet users on their computer as well as their mobile devices. At Golden Frog, we control our network, own all the components, and therefore do not rely on outsourced or third-party hosting sites to deliver our service. We own the Garden of Eden, and the Tree of Knowledge is open to everyone.

“Innovation is the central issue in economic prosperity.”

*Michael Porter*

VyprVPN is a personal virtual private network (VPN) that protects an individual's privacy on the Internet and prevents Internet service providers from monitoring or controlling online communications and activity. The VPN allows users to access certain websites that may be blocked in restrictive countries. VyprVPN is Golden Frog's attempt to protect netizens from the big dog Internet companies like Time Warner and AT&T. But more than that, it is our answer to the Internet's Second Amendment promise of encryption.

Cyphr is an easy-to-use, zero-knowledge encrypted messaging app. This means Golden Frog cannot read, decrypt or share your messages. Cyphr generates a unique public and private key pair so only you and your friend can read your conversation - not us, not your wireless provider and not third parties.

The tools were designed for the user and to benefit the user directly. We do not mine users' personal data and share with third parties. We continue to develop new applications to advance the cause and make it possible regardless of what governments and regulatory bodies decide to do. Our commitment to application innovation will ensure that the Internet remains open and free.

And we believe all companies should do the same. Government decree and corporate regulatory policies can only limit growth and opportunity. The only way to manage potentially dangerous or inappropriate content is to allow users to self-regulate and adopt innovative solutions to ensure their own protection.

# Humanity is an Ocean

It covers 140 million square miles and nearly 75 percent of the Earth's surface. It connects us to each other, across language, and culture. It sustains life and supports life.

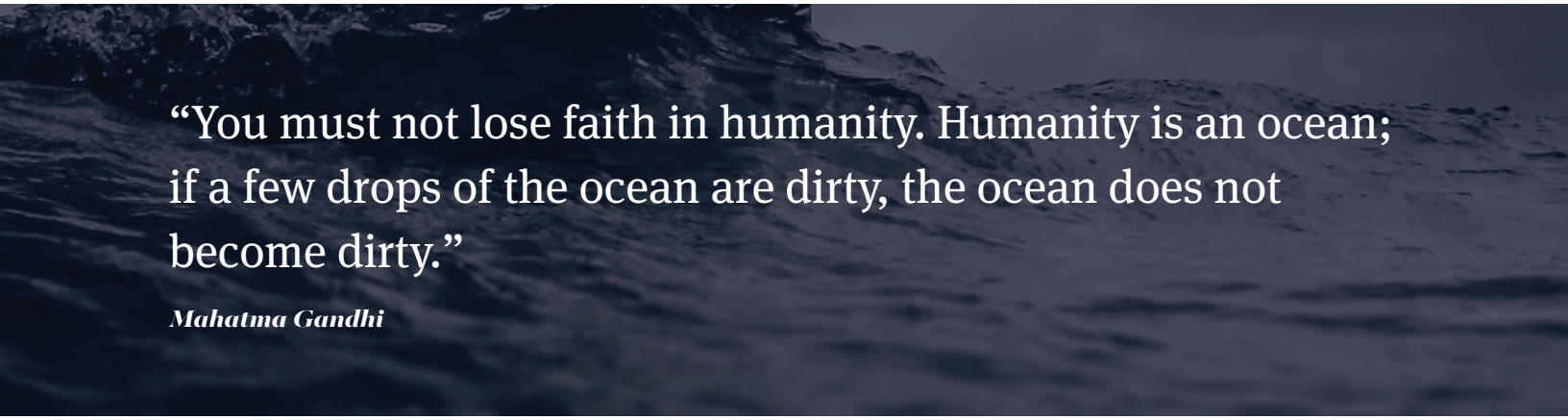
Our climate and the quality of the air we breathe depend on it. Throughout

history, it has served a primary role in trade and commerce, exploration and discovery.

It is the ocean.

Like the ocean, the Internet now connects us despite language or culture. The Internet has become the foundation of commerce and trade, exploration and discovery. And just like the ocean, there is danger and pollution.

But despite these problems, we understand that the ocean, in all its wonder, is good. That one drop of dirty water does not destroy what binds and connects us across continents. And so too does the Internet.




The oceans have long been subject to the freedom of-the-seas doctrine—a principle put forth in the seventeenth century essentially limiting national rights and jurisdiction over the oceans to a narrow belt of sea surrounding a nation's coastline. The remainder of the seas was proclaimed to be free to all and belonging to none.

Like the ocean, the Internet connects people. It is a sea of ideas, commerce, connections, relationships and consciousness. The Internet facilitates communication, transactions, innovation, identities, entertainment, educational growth and enlightenment.

Like the ocean, the Internet must remain open and free. Humanity is an ocean. A limit on the Internet is a limit on humanity and its promise for the future.

Many people and groups challenge our online freedom by controlling content on websites or limiting access altogether. These restrictions do not support freedom or enable our global society to flourish. Whether the reasons to restrict online access are preventative or a reaction to criticism, an open Internet cannot endure if companies and individuals continue to inhibit access and limit sharing of information.

While regulation of the underlying transmission is necessary so that competition is possible, Internet access providers should be allowed to charge for access and provide services in a free market. Consumers have choices in a free market and have the right to use or decline services or applications. The Internet is and should continue to be a free market of ideas and information and be accessible to everyone who wants to use it from any part of the world. As legislation that could potentially threaten our freedom progresses through Congress, we must all stay informed and be active proponents of an open and free Internet.

Innovation helps drive economic growth and helps maintain a free and open Internet that has no borders or limitations. The appropriate and effective solutions are available and more will be developed.

Netizens of the world must arm themselves with the tools to protect their information and identities online. A global commitment to a free and open Internet will help us foster global prosperity and promote peace.

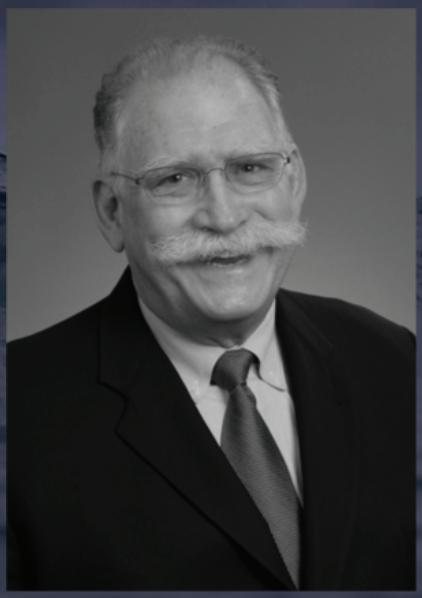
We ask that you join a growing, global movement of people committed to a purpose—a cause—to defend, promote and ensure that the Internet remains open and free.

This cause is not merely a fight to ensure free speech, but it is a strategy for global commerce, international understanding and ultimately peace and prosperity.

**LIKE THE OCEAN, THE INTERNET MUST REMAIN OPEN AND FREE**

# About the Author

*Ron Yokubaitis is the Co-Founder and Co-CEO of Golden Frog.*



A native Texan and 40+ year resident of Austin, Texas, Ron has held a lifelong passion for electronics and communications—first fueled by obtaining a ham radio license more than 40 years ago. While that made the world smaller for him, it was his discovery of the Internet that truly opened his eyes to the possibilities. He first learned of the Internet in 1976 from Steward Brand's book, "Cybernetics Frontiers II" and attempted to log on for the first time in 1984 at an Artificial Intelligence Conference at the University of Texas in Austin, TX but was refused access.

In 1994, Ron recognized the lack of Internet access options for the "unwashed"—those who were not a student or government employee. In response, he and his wife, Carolyn Yokubaitis, co-founded Texas.net—one of the first 50 ISPs in the United States. Focused on providing Internet services dedicated to customer privacy and security, Ron and Carolyn's investments in Internet businesses have grown and expanded into multiple businesses including Giganews, the world's leading Usenet provider with users in 215+ countries, and Data Foundry, a global provider of data center colocation, managed services and disaster recovery services.

Golden Frog is the latest venture established by Ron and Carolyn and is committed to developing applications and services that preserve an open and secure Internet experience while respecting user privacy. Golden Frog's two products, VyprVPN and Cyphr, currently have customers in 215+ countries. Golden Frog owns and operates its own global infrastructure with private server clusters in North America, South America, Europe, Oceania and Asia.