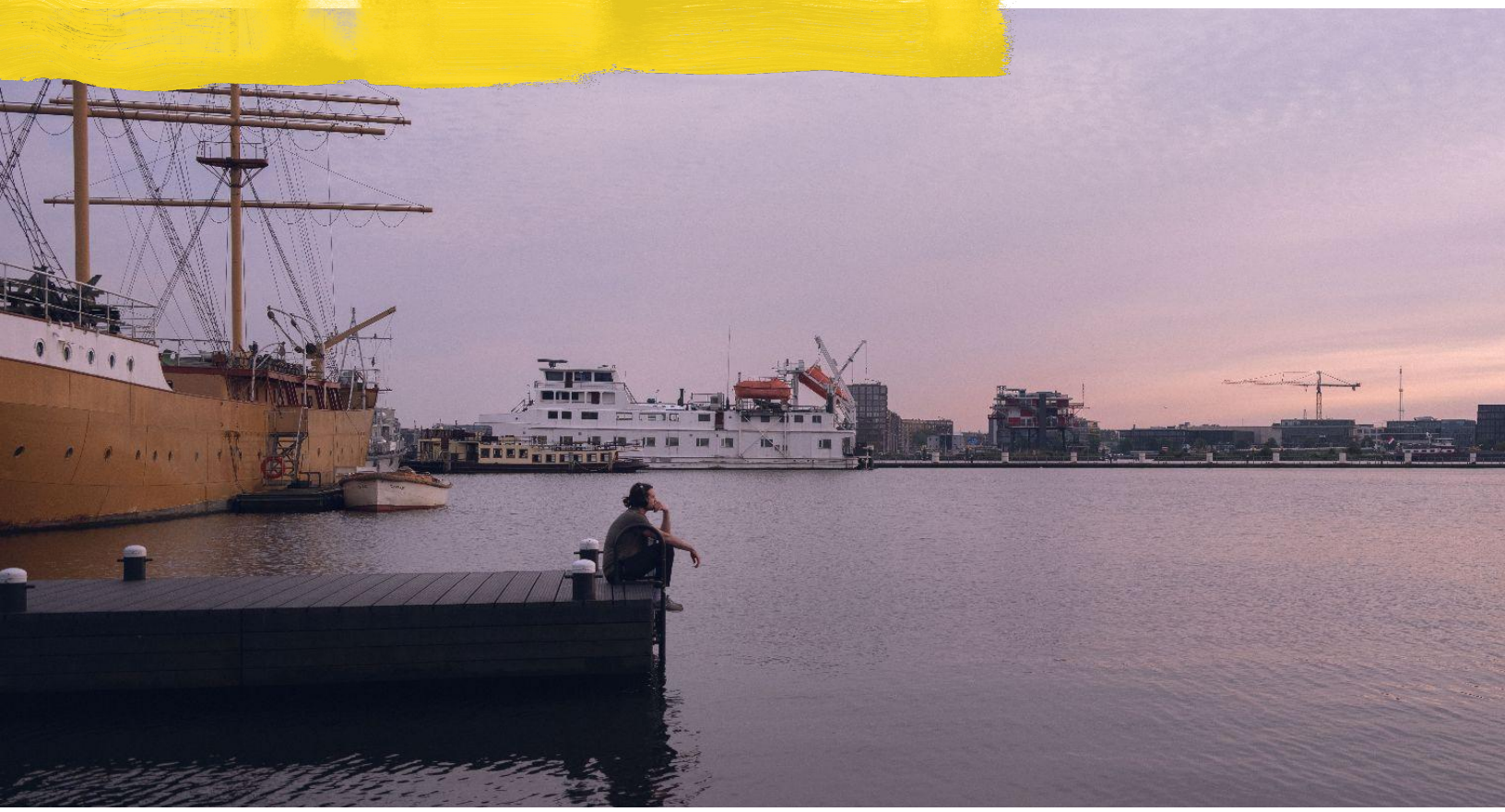
Stellar

THE CASE FOR OPEN SYSTEMS: CREATING AN INTEROPERABLE, INTEGRATED WORLD

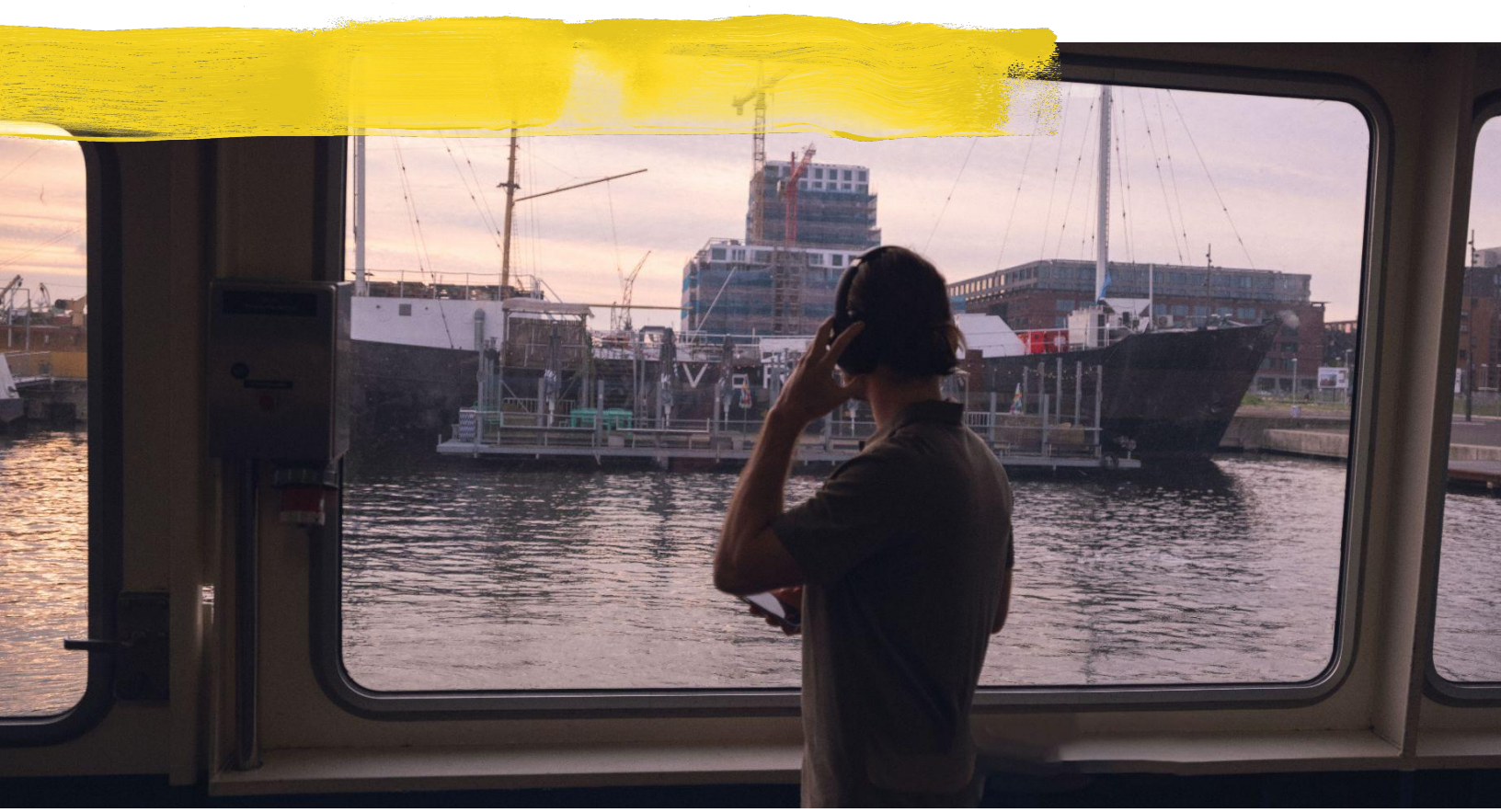


The concept of open systems, popularized in the 1980s, emerged as a solution to address an increasingly fragmented landscape in the technology sector. The term was primarily used to describe the Unix operating system, which emphasized standardized program interfaces and encouraged the use of third-party hardware and software. At the time, this was a novel concept; many technology firms had created their own proprietary computers and accessory equipment, none of which were compatible with one another. Purchasing an IBM computer, for example, meant that an individual could only use IBM's peripherals and equipment. In the early days of modern computing, vendors enjoyed this competitive advantage but quickly realized that customers were dissatisfied with the lack of flexibility and the siloed nature of the technology industry. This dissatisfaction spurred some developers to advance an open system philosophy as a way to encourage standardization and cooperation, in the hopes of creating widely interoperable, integrated technology components.[1]

[1] Huston, "Reexamining internet fragmentation."

Today, open systems have become an unofficial standard for how many essential technologies work–the Internet is an example of a system that adopted common standards to optimize performance and behavior. In fact, many industries continue to work towards a more standardized ecosystem. For example, SWIFT–a global messaging network for financial institutions–is adopting a new messaging repository to use among financial institutions. This initiative is creating a universally adoptable, open-source platform with data-sharing capabilities to improve cooperation among financial institutions.[2] Yet critics argue that open systems are subject to vulnerability to security breaches, slow and inefficient decision-making, and the potential for inconsistent, unreliable, or poor quality system developments.[3]

Should policymakers allow the pendulum to swing back towards closed systems in light of these criticisms? To answer that, it is important to consider the implications of a world in which technology is siloed. In closed systems, software development is privatized, user data is created and controlled by only a handful of major corporations, and applications, hardware, and content are subject to "walled gardens"–an environment in which a technology provider exerts significant control and suppresses consumer choice. These conditions lead to a narrow playing field where a few institutions wield disproportionate power and stifle innovation from smaller competitors. Once power is consolidated, it becomes increasingly difficult to dismantle, as seen in the current state of the technology sector, in which a select number of mega companies dominate much of the landscape. Consumers and policymakers alike therefore depend on a world that allows for and encourages connected, essential technology. To do so requires embracing an open system philosophy that promotes interoperability, integration, and compatibility as technologies grow and scale.

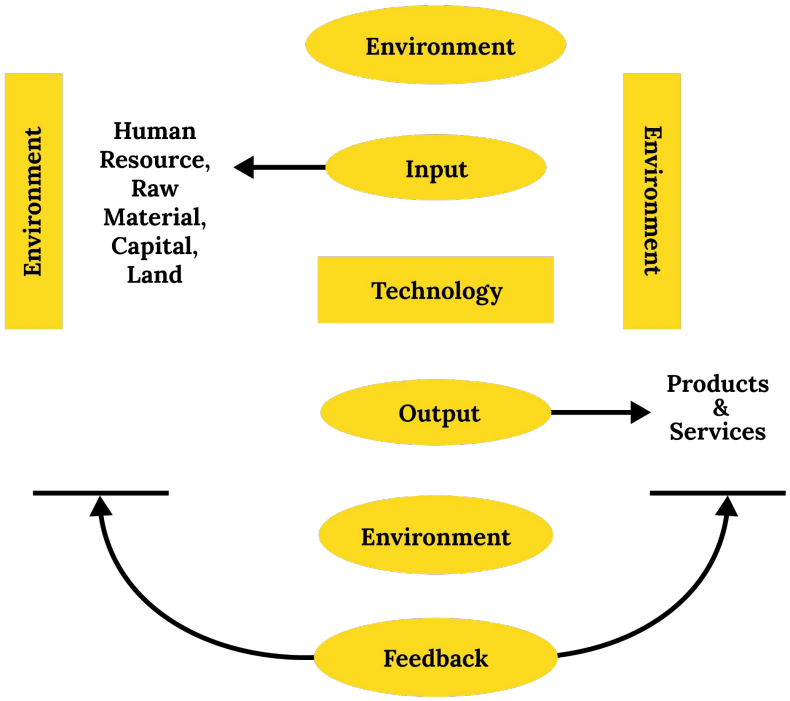


[2] ISO 20022 Registration Authority, "APIs and ISO 20022."
[3] O'Neill, "The Internet runs on free open-source software. Who pays to fix it?"

I. WHAT IS AN OPEN SYSTEM?

An open system is broadly defined as an operating model that allows its environment to participate in defining and developing the purpose of that system. In other words, an open system allows for the flow of information between the system and its larger environment, and for the system to adapt based on that exchange. In scientific literature, for example, the term "ecosystem" describes the interactions and interdependencies among organisms that collectively enable their system to function. Similarly, in today's digital world, open systems are neutral platforms that create opportunities for collaboration and engagement among their technology-utilizing members.

Figure 1: Example of an open system environment



Source: CIO Wiki

An open system accomplishes this goal through three interrelated philosophies: Open Source, Open Access, and Open Data. Although each of these three philosophies has its own characteristics, they share many important commonalities that provide necessary redundancies in a resilient open system. Members of an open system work together by agreeing on standards to reduce software fragmentation, sharing network infrastructure to improve service delivery, and sharing data to build better services. Although applying the open system philosophy broadly may be novel, the importance of an open system is not. A common, interoperable, and flexible environment is critical to the future of systems design to ensure equitable, diverse, and accessible participation and control. But to achieve this, an open system framework should be implemented from the outset. Converting retroactively to an open system can be difficult for institutions that face issues such as license lock-ins and lack of transition support.[4] Systems also have a tendency to become more closed over time, so it is important to establish guidelines from inception that support and reinforce openness.

[4]Instaclustr, "New Study on Open Source vs. Open Core Trends Shows Increasing Demand for Open Source's Advantages."

Box 1: A brief history of the Internet

The Internet, originally created by the U.S. Department of Defense, remains an important example of standardization and open system design. For instance, anyone can develop and create applications built on top of the Internet. Today, the Internet services an interconnected network of systems ranging from computers to smartphones. However, network communication in the early days of the Internet was limited to servers that required previously established connections between terminals. Each network terminal had its own set of user commands and could only communicate with a particular party.[5] The invention of ARPANET–the first workable prototype for the Internet we know today–was revolutionary because it allowed a terminal to communicate with multiple systems using a single network and a common protocol.[6]

This networked approach demonstrated the power of an open system in fostering collaboration, eventually leading to the development of the Hypertext Transfer Protocol (HTTP). HTTP, a protocol for exchanging information over the Internet, set the standard for webpage development and spurred the mass adoption of Internet-based technology. This protocol serves as the basis for seamless access to the Internet and Internet-based applications from any device, anywhere. However, the Internet is not as open as it once was. While the Internet is still considered an open system, a small group of players controls a significant share of applications, servers, and data.

Early system design was driven by hardware engineers and their critical developments, resulting in closed ecosystems that favored proprietary technology to foster competition. As the industry matured, hardware became more standardized, and competition shifted to novel software tailored to the diverse needs of users. Today, services focus not only on users but also on how users can interact with a larger application environment. Digital services now build platforms that create environments to bring users together.[7] The digital economy is increasingly disintermediated and creating new peer-to-peer interactions, which means platforms grow through both direct and indirect network effects.[8] A strong user base encourages more users to join a thriving platform and separately attracts skilled developers as well.

[5]University System of Georgia, "A Brief History of the Internet."
[6]Wright, "What Is ARPANET and What's Its Significance?"
[7] Zhu and Iansiti, "Why Some Platforms Thrive and Others Don't."
[8]Ibid.

Box 2: An example of a closed system: Apple

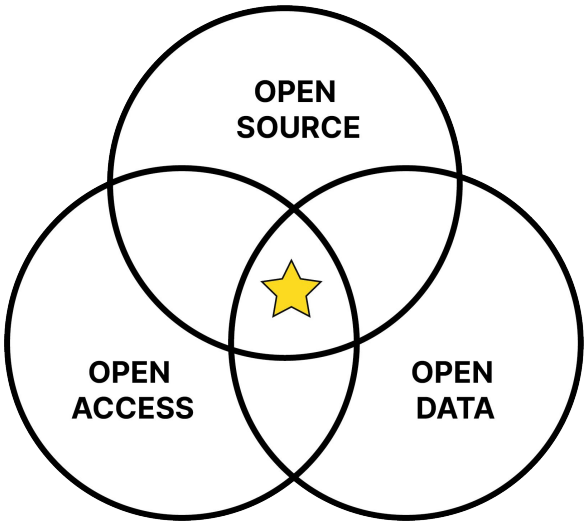
In practice, closed systems exclude participation and hinder innovation. The Apple universe is a well-known closed system and is considered a classic "walled garden" because its products make it difficult to switch vendors. This leaves many decisions at the discretion of the company and creates proprietary software that is incompatible with other platforms. Apple ultimately benefits from this at the expense of consumers. One consequence of this closed system is monopolistic behavior. In 2022, the average price of a smartphone worldwide was $299, while the iPhone 12, Apple's most affordable line, started at $599. Apple also has the power to decide which applications are available in its ecosystem and how they are used. For example, the popular video game Fortnite is currently banned from Apple's App Store because it allowed users to spend money in-game without using Apple's App Store. Apple's closed system also makes its hardware and software incompatible with products outside its ecosystem. In another instance, Apple exercises discretionary power over otherwise universal hardware such as charging ports. The EU has even required Apple to standardize its iPhone charging port to match all other phones.[9] In contrast, the open system of Android, Google's mobile operating system, continues to expand the number of external system participants. Windows users can mirror their Android phones on their desktop, even though they are different companies with different software.

Consumers and end users stand to benefit considerably from open system environments, as they promote important features such as interoperability and diversion of power from a centralized entity. The design of systems is therefore an important consideration for policymakers who will help shape applications and their environments in this new digital age.

[9]Guarascio, “Apple Forced to Change Charger in Europe as EU Approves Overhaul.”

II. THE SUM OF ITS PARTS

Figure 2: Components of an open system



WHAT IS OPEN SOURCE?

Source code is the fundamental building block for digital programs and undergirds the core functions of all software. Open systems are powered by source code, but designate code as open-source. Under definitions maintained by the Open Source Initiative–the steward of the Open Source Definition, the set of rules that define open source software–an open-source license allows anyone to freely use, modify, and redistribute software based on open-source code.[10] Among these rules, some are particularly important to note: the source code must not be intentionally obfuscated, the license must allow derivative works and their distribution, and the license must not set parameters that restrict derivative software. In contrast, proprietary software is developed behind closed doors and is subject to strict licensing restrictions that prevent others from accessing and developing the source code. The benefits of open-source software continually shape how the Internet is used: two open-source web servers, Nginx and Apache, account for over 60% of all websites on the Internet.[11]

Open-source software is important for businesses, developers, and users because it enables fast, flexible, and robust development and security that leverages community-driven guidance and expertise. Open-source programs are commonly built on an array of prefabricated source code, so builders can focus on more advanced developments rather than investing time in designing a program's fundamental features. Standardized and open-source code also allows community users and developers to directly affect software development and make changes without waiting for vendor-led updates. Because open-source code is not limited by vendor constraints, developers can build products that are well-suited to user needs by making necessary changes themselves. In fact, the longevity and usefulness of open-source projects underpin much of existing technology and applications. The Linux Foundation estimates that free and open-source software constitutes 70-90% of any given modern software.[12]

[10] Perens, Sroka, Stu, "The Open Source Definition."
[11] W3Techs, "Usage Statistics and Market Share of Web Servers, August 2023."
[12] Perlow, "A Summary of Census II."

Box 3: An example of open-source software: Chromium

Open-source software provides a backdrop for extensive development by user communities. An important example is the release of Chromium, the open-source code for Google's proprietary browser Chrome. This release led to the development of many other popular browsers that are now compatible with various operating systems. For instance, while Chromium has minimal privacy features, browsers built on Chromium have additional features like website and location permissions. As of May 2023, Chromium browsers accounted for nearly 71% of the browser market share, with users using Chrome, Microsoft Edge, and Opera. Even though Google is the primary backer of Chromium, the project's open-source nature allows anyone to modify and use its code. Google competitor Microsoft, for example, has provided input to the project since 2019.

Open-source code is also enterprise-independent and permanent. By existing independently of any one group of developers, platforms that use and create derivative products do not have to worry that software will no longer be supported–a major concern from both a usability and a security perspective. Unsupported software means that developers no longer provide patches, fixes, or updates to software, leaving systems open to vulnerabilities and posing security risks for end users and their information.[13] For example, the WannaCry ransomware attack in May 2017 targeted legacy Microsoft operating systems that had reached end-of-life. One of the largest institutions affected was the National Health Service hospital system in England and Scotland, which at the time of the attack had thousands of computers running Windows XP, an operating system that had not been updated since 2014.

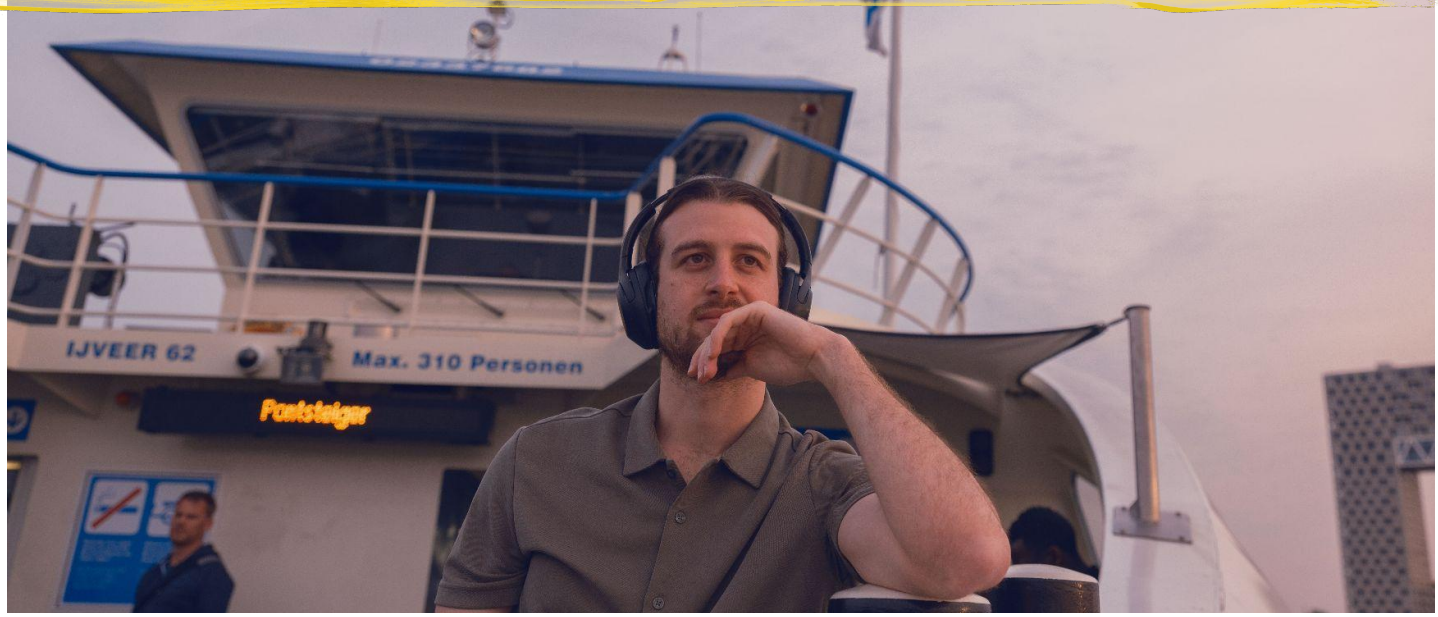
In general, the safety concerns and protection of open-source and proprietary code do not differ significantly. Companies and contributors have a common interest to keep projects secure, which requires similar necessary precautions for both open-source and proprietary code. In fact, the National Institute of Standards and Technology, a U.S. government agency that develops, promotes and maintains metrics and standards for several industries, created guidelines highlighting best practices for securing software that apply to both open- and closed-source code.[14] Further, proprietary software does not guarantee security and is often not more secure–in 2022, a hacker group called Lapsus$ stole 90% of Microsoft Bing's source code.

[13] Prozac, "5 Security Issues From Using an Unsupported Operating System."
[14] Black, Guttman, Okun, Black, Guttman, and Okun, "Guidelines on Minimum Standards for Developer Verification of Software."

Open-source code has one specific advantage over proprietary code when it comes to security: open-source relies on a network of community contributors that can subject code to more rigorous scrutiny. Researchers from Microsoft and the U.S. Department of Homeland Security concluded that open-source code reinforces sound security practices because it involves many people who can quickly expose bugs and provide reusable, secure, and working code.[15] They maintain that proprietary software patches are often slowed down by process flows while the open-source community can implement fixes faster. The open-source community is not simply a group of hobbyists; the popularity of open-source projects means corporations have vested interests and employ experts who are also devoting their efforts to finding and fixing issues. While improving security and reliability by relinquishing control of a system to a network of individuals may seem counterintuitive, community-led responsibility is a critical feature of open systems. Both users and systems benefit from collective innovation by receiving access to resilient, customized, and secure applications.

WHAT IS OPEN DATA?

Open data is data that can be freely used, reused, and distributed in a way that is universally appropriate and modifiable.[16] Open data can include public data collected from government agencies to information on consumer behavior from the private sector. In all cases, data excludes any information about or can be traced to specific individuals; sensitive data subject to security restrictions is also excluded. Data is always created when users interact with programs and applications and an open data philosophy promotes robust accountability and transparency of this information. This is achieved by offering access to and auditability of the data, which in turn creates opportunities for accountability and research to identify and address issues. OpenSpending, for example, is a platform where governments and civic organizations can publish their revenue, budget, and procurement data.[17]



[15] Clarke, Dorwin, and Nash, "Is Open Source Software More Secure?"
[16] Perens, Sroka, Stu, "The Open Source Definition."
[17] Open Knowledge Foundation, "OpenSpending."

Consumers also regularly voluntarily share their data with third parties for unintended and unknown purposes. When users consent to share their data, they may lose the right to know where data is stored, what it is used for, and under what conditions it is shared. Consumer data has become a valuable asset that many organizations in both the public and private sectors rely on for decision-making. In the private sector, data strengthens market positions and creates barriers for new entrants, extending the reach of incumbent Big Tech firms.[18] Internal documents from Amazon in India show that Amazon used proprietary data to launch its own version of products that were identical to competitors' products and manipulated search results to promote Amazon's own version of a product over the competitor's.[19]

Using data to manipulate consumers and markets is common practice with firms that retain and profit from the information. This behavior can lead to compromised markets and encourage monopolistic behavior through a private data-network activity loop.[20] Here, data is mined to create features that benefit from network effects, which in turn increase user activity and generate more data. While beneficial in an open system, this feedback loop in a closed environment concentrates power and stifles competition by farming important data and limiting its visibility for industry-wide innovation. Open data is necessary to build large, complex systems without creating unproductive and anti-competitive behavior.

One example of an initiative that is redefining how legacy institutions use their data is the open banking initiative. Bank data from traditional institutions has been historically difficult to share: individuals can download and access their data, but that data cannot be transmitted to other financial institutions or used meaningfully. Under open banking, participating banks share information like transaction history with independent third-party providers that participants can access. Open banks empower consumers to use their transaction data in ways they were previously unable to and help connect lenders to more borrowers, creating a more vibrant, competitive market.

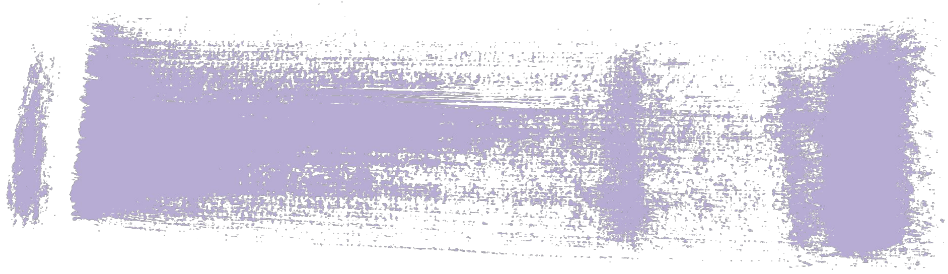
[18] Venâcio, "Why Data Monopolies Matter."
[19] Kalra, Stecklow, "Amazon Copied Products and Rigged Search Results, Documents Show."
[20] Shin, "Big Tech in Finance: Opportunities and Risks."

Box 4: Nubank and the application of data

In Brazil, Nubank is an important example of a company focused on transforming an industry that historically had failed to use customer data in the best interest of the customers. Although there are over 150 commercial banks in Brazil, five banks account for 87% of all commercial bank assets.[21] In 2017, only 15% of citizens from the poorest 40th percentile borrowed from a formal financial institution.[22] Banks offered few credit options and also charged high-interest rates – in 2017, the lending rate was 46.90%.[23] Banks cited high delinquency rates, operating costs, and lack of consumer data for their high fees.

When Nubank launched its lending business, it used data from credit bureaus and its own data on consumer spending patterns to make data-driven decisions. Nubank offered introductory loans starting at $14 and automatically offered higher credit limits as a customer's credit history grew.[24]. This is in contrast to commercial banks that charge high interest rates to hedge against consumer uncertainty and require extensive credit history before extending loans. In 2022, Nubank joined Open Finance, an initiative of the Central Bank of Brazil to promote the sharing of data, products, and services between regulated financial entities. This service allows customers to take their financial history to any participating bank. For example, if another bank offers a more favorable lending term but does not have enough individual banking history, a customer can freely share their data with the participating bank.

In practice, one way open data can provide value to industry and consumers is through application programming interfaces (APIs). APIs are a set of protocols for building and integrating applications such that information, like data, is shareable and usable. While privatized data is useful in their own siloed environments, they offer little value otherwise. The ability to combine data to have access to more diverse and comprehensive datasets creates real value for consumers.



[21] Federal Reserve Economic Data, "5-Bank Asset Concentration for Brazil."
[22] World Bank, "The Global Findex Database 2021."
[23] World Bank, "The Global Findex Database 2021."
[24] Kauflin, "How David Vélez Built The World's Most Valuable Digital Bank And Became A Billionaire."

WHAT IS OPEN ACCESS?

Open access puts the focus on underlying infrastructure, and separates the provision of networks from the provision of services. This allows network providers to focus on robust and extensive network development that supports not only the rights to services but also the means to receive them. As such, the goal of open access networks is to ensure that individuals have both availability and accessibility to services built on open-source and open data. An open access environment achieves this through two defining characteristics: equitable access and the inability of any single entity to significantly control the environment. Individuals can elect to participate in necessary operational and decision-making roles, distributing decision-making power among all system participants and preventing centralized control. This separation of provider responsibilities also mitigates the potential for perverse incentives from network providers who offer services on their own network.

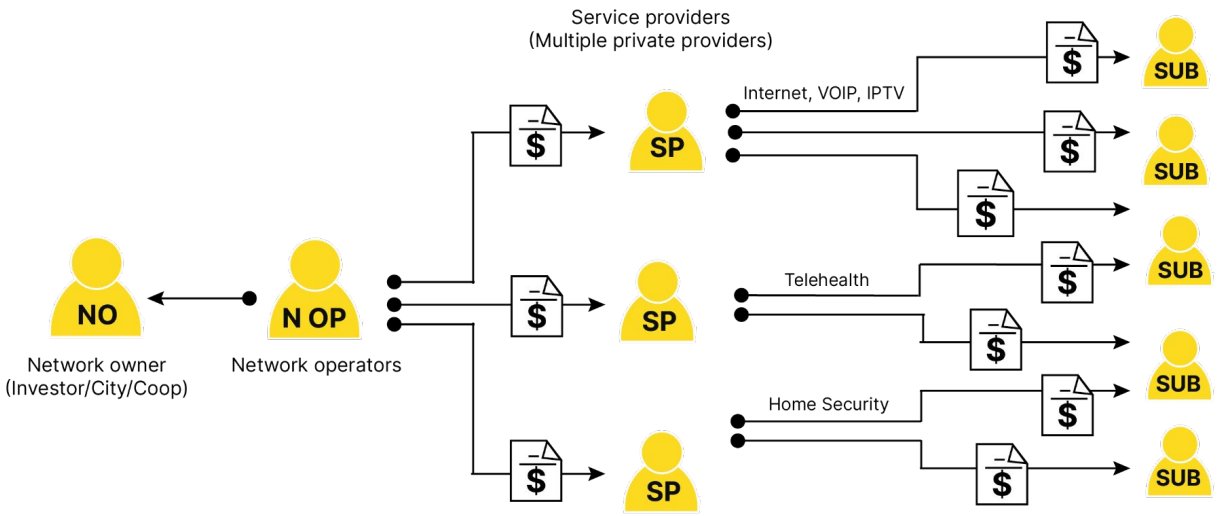
Box 5: An example of open access networks: Wired Road

Traditionally, telecommunications operators have sought exclusive access to their networks, making it costly to expand into rural areas that require high labor and offer low returns and precluding many communities from Internet-based services. Open access networks, commonly provided by a conglomerate or an institutional network provider, offer a solution by creating a shared network that service providers can use. This allows multiple Internet service providers to use the same infrastructure to provide Internet access, addressing the last-mile challenge. One example of this initiative is Virginia's Wired Road, a shared network on which service providers that meet minimum technical requirements can operate.[25] Wired Road does not sell any services itself; users purchase services directly from service providers. Open access networks like Wired Road can reach and provide services to those forgotten or unreachable by existing services. They provide new and faster ways to send and receive services, payments, and products. Wired Road is not a unique case; in fact, many municipalities and regions utilize shared networks to provide access to their residents.[26]

[25] The Wired Road Authority, “About The Wired Road.”
[26] Institute for Local Self Reliance, “Welcome to Community Networks.”

While open access networks are mostly used in the telecommunications industry, this model is relevant and equally as important to other infrastructure corridors as well. One important application is public, open access blockchains. These infrastructures are neutral platforms that anyone can use and are maintained by unaffiliated, independent developers who are interested in supporting the network's infrastructure. Service providers can then build additional features with users in mind, focusing on issues such as improving transaction speed. This creates competitive markets, which are known to lower costs for users and barriers to entry. In both the digital and real world, open access networks create competitive marketplaces by aligning incentives and focusing efforts. Service providers innovate to compete for users and network providers focus on building resilient, effective infrastructure to attract service providers.

Figure 3: Example relationship between network and service provider



Source: COS Systems

III. PROTECTING AND PROMOTING OPEN SYSTEMS: THE ROLE OF THE PUBLIC SECTOR

Taken together, the components of open systems–open source, open access, and open data–create interoperable, connected technology and build the foundation for greater transparency, innovation, and competition. An open system philosophy can ensure equitable access for users and democratic governance over environments without the possibility of outsize influence. Yet many platform-based companies still operate in closed-system environments that give them complete discretion over user data and encourage adverse effects like anti-competitive behavior and consolidated market power.[27] It is important that system operating models be updated to adequately address and reflect today's technological advances.

Supporting further development of open systems should therefore be an important priority for governments around the world, particularly the United States government, as open systems accomplish many key public policy objectives: promoting operational resilience, encouraging improved access to services, and empowering users to exercise more control over their data. Further, an open systems philosophy can ensure equitable access for users and democratic governance of those systems. Open systems make information like user data and source code easily accessible, and communities can leverage this knowledge and innovation to make more informed decisions.

The following recommendations are designed to support U.S. policymakers in their efforts to encourage the growth and development of open systems:

- → ***Develop U.S. government expertise.*** *T*he U.S. government should build human capital within relevant federal agencies and departments on open systems through training and professional development opportunities, including rotational assignments in private sector companies that build on and/or contribute to the maintenance of open systems. This type of first-hand, technical experience and learning is essential to fostering a baseline proficiency in open systems among career civil servants.
- → ***Provide clear, standardized dataset classifications that indicate confidential and sensitive information.*** U.S. policymakers should ensure that open systems actually improve outcomes and do not endanger individuals and organizations. Clear guidelines should be presented to prohibit the release of sensitive and personally identifiable information. Organizations that build in open system environments should also maintain certain intellectual property rights to accommodate for continued open-source development. Standardization is also important to establish and maintain a common understanding of data classification.
- → ***Support the creation of public projects.*** Projects that encourage public participation like Open Data DC support the creation of community-led data-based applications and use cases. U.S. policymakers should support the creation of other similar engagement opportunities that drive practical use cases that help support the adoption of open systems design.

[27] Federal Trade Commission, "Monopolization Defined."

- → ***Promote interoperability as a significant federal prerogative.*** U.S. policymakers should identify areas that could benefit from greater interoperability and common technical standards, such as data portability, message forms, and digital identity, and develop policies that promote the use of open formats and protocols in public projects. Sound policy should also maintain interoperability both within and between systems to prevent the formation of walled gardens.
- → ***Encourage public-private partnerships.*** Greater engagement among industry, academia, and the U.S. government on open systems will support discovering use cases for open system environments. Encouraging this open dialogue will facilitate an exchange of information and lead to better policy outcomes. To do so, relevant U.S. governments and agencies, such as the Department of Commerce and the White House Office of Science and Technology Policy, can stand up working groups that formalize public-private cross-collaboration.
- → ***Accelerate grant funding toward open system initiatives.*** The U.S. government is already a major source of funding for scientific and engineering research and development (R&D).[28] Increasing the share of R&D from agencies and departments, like the National Science Foundation and the Department of Defense, toward open source projects and initiatives would bolster the growth and development of open, integrated data and knowledge infrastructure that could benefit private industry and maintain the United States' competitive edge internationally.
- → ***Drive the international agenda on open systems.*** The U.S. government has a critical leadership role to play in shaping how allies and international organizations and standard-setting bodies view open systems. U.S. advocacy for open systems on the global stage would encourage the development of worldwide standards on interoperability and compatibility that support open system development and promote more democratic access to technology.

While the components of an open system are not novel, the sum is indeed greater than its parts. Open systems represent the amalgamation of individual philosophies to create new operating environments built on novel forms of web-based infrastructure. Terms like Web 3 and open governance try to capture this innovation and emphasize the value of open systems in promoting equitable access, consumer protection and innovation, and representative decision-making. With many initiatives already taking place in the private sector, policymakers ought to appropriately consider this iteration of platform-based systems design and ensure that it is given the space and support needed to develop and innovate.

[28] Congressional Research Service, "Federal Research and Development Funding: FY2023."