COMMUNAL INTERNET INFRASTRUCTURE

AN ALTERNATIVE, SELF-MANAGED APPROACH TO DIGITAL SPACES BUILT UPON VALUES OF COMMUNITY, AUTONOMY & COLLABORATION

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

EXECUTIVE SUMMARY

This paper explores the concept of communal internet infrastructure – an alternative, self-managed approach to digital spaces built upon values of community, autonomy and collaboration. Unlike traditional corporate or government-controlled networks, communal infrastructure is designed, owned and operated by the community or organisation it serves, emphasising democratic management, privacy and user rights.

This document is meant to serve as a foundational guide to understanding and implementing communal internet infrastructure, highlighting its importance for empowering communities to take control of their digital lives in a secure, private and values-aligned manner.

INTRODUCTION

Autonomous, self-hosted, feminist, alternative, self-managed: these are just a few of the terms used to describe internet infrastructure that reflects particular values, principles and collaborative ways of building, managing and inhabiting digital spaces. APC's relationship with infrastructure dates back 35 years, when a group of visionary technologists – who also saw themselves as environmentalists – recognised the immense potential of emerging telecommunications systems. They envisioned infrastructure that could be owned by and serve the people. Hardware and software became the new roadways, the intercontinental bridges for communication, interaction and engagement.

We believe that origin stories matter. They provide context and help shape the collective understanding of something that, once introduced to the world, grows, evolves and transforms its ecosystem. APC has always centred its work around the idea of the internet and digital technologies to be managed as commons, as "people-owned" infrastructure. As we explored these ideas further, analysing the current internet infrastructure trends, we arrived at the concept of "communal internet infrastructure" – the broadest, most inclusive concept for it that encompasses the following possible features:

- Used or shared in common by a group
- Belonging to the people of a community, and shared with or participated in by the public
- Pertaining to a community
- Engaged in by or involving multiple communities.

This paper has been developed by the Communal Infrastructure Working Group of the Association for Progressive Communications (APC). It is born out of our own experiences, as well as those of APC members and partners. We are particularly grateful to the participants in a session at APC's Community Gathering in Thailand in May 2024, whose insights provided a valuable conceptual base for this piece.

We hope this marks the beginning of a series of papers in which we can further explore the details of implementing specific projects, as well as fostering further developments in this area.

HOW WE UNDERSTAND COMMUNAL INTERNET INFRASTRUCTURE

While we recognise that not every solution based on communal infrastructure has to be connected to the internet, we will centre this paper on infrastructures belonging to the interconnected online realm. However, it is also entirely possible to build powerful local communal infrastructures disconnected from the global network and serving only the directly surrounding community, including technologies like local radio stations or community networks with local content repositories. By nature, these types of technologies are closely linked to communality and can serve as inspiration to rethink global internet-connected infrastructures.

When we develop infrastructure to work and participate in online spaces, we rely on several layers of components including hardware, software, policies, norms, people, systems, connectivity and rules; they all constitute parts of the internet infrastructure needed to access the different services. Often without realising it, the decisions we make – or don't make – about the technologies that enable online interactions can significantly impact our online rights.

So here is our definition:

Communal internet infrastructure refers to the combination of agreements and relationships that together with hardware, software and applications are used in order to provide one or more internet-based services, and that are designed, owned/co-owned, managed and operated by an organisation or community. The resulting services are conceived and operated with a people-centred approach, taking into account equitable and rights-respecting guidelines.

Some takeaways from this definition include the following basic concepts:

People-centred:

The design of the solution has as its centre the people, their context, experiences, accessibility needs and knowledges. In these models human relationships matter, and are key to the way the infrastructure is understood, perceived, sustained and accessed.

Inclusive design:

There isn't a one-size-fits-all solution for communal infrastructure; different communities require different approaches tailored to their unique needs. What defines communal infrastructure is the intentional design and operation that align with the community's values and requirements.

Co-responsibility:

Different communal internet infrastructures can have varying levels of "user" participation in decision-making processes and a varying share of their responsibility and knowledge in maintaining the infrastructure. While it is encouraged that the "users" take part in defining the services they use, in some circumstances this might pose an additional burden. Still, communal infrastructure should encourage and facilitate user engagement and should not pose obstacles if the users want to gain knowledge about technical aspects or have a say in decision making. In contrast to what happens with for-profit models like corporate services, users of communal infrastructure should play a part in caring for the infrastructure, as well as using the services mindfully of environmental impact. This is a significant step away from the extractivist mindset towards one of co-responsibility and care.

Community ownership:

The solution encompasses the diverse technical components necessary for people to access the internet, maintain an online presence, and operate online services for themselves and others. In a well-defined communal infrastructure, the selection of these components is driven by the specific needs of the community and operated in a people-centred way. This infrastructure is operated transparently and efficiently, with a strong emphasis on protecting the privacy, safety and rights of users and their dat

Communal infrastructure **doesn't have to offer services free of charge**; it can also be used to provide paid services, depending on the community's chosen model and resources.

WHAT IS NOT COMMUNAL INFRASTRUCTURE

Understanding what is **NOT** communal internet infrastructure can help clarify its unique characteristics and importance. Here are some key distinctions:

Commercial cloud services that are privately owned and operated, often with limited transparency or input from the communities that rely on them.

Corporate internet service providers (ISPs), i.e. traditional ISPs that operate as private entities driven by profit. These companies own and control the network infrastructure, make decisions based on corporate interests, and often have little direct accountability to the communities they serve.

Top-down government-controlled network infrastructure, like data centres, where the government directly controls internet infrastructure, often using it as a tool for surveillance, censorship or propaganda.

Data monetisation services that might offer charge-free services, but rely on harvesting and monetising user data.

To summarise: Communal internet infrastructure is distinguished by its community ownership, democratic management, and focus on people-centred rights and privacy. It contrasts with private, corporate or government-controlled networks, where the primary focus is on profit or centralised control, often at the expense of the users' needs and rights.

WHY COMMUNAL INFRASTRUCTURE IS IMPORTANT

Most people connect and interact online with each other using online services without giving much thought to important questions like: Where is my data being stored? Who has access to my information? Am I being tracked? To what extent can I own and control my information? These concerns often only come to mind when something goes wrong, such as when data is blocked, compromised or used against the person.

When a community or group of people own the infrastructure, they gain the power to define and control the mechanisms that protect their services and data. This ownership brings several key advantages:

Autonomy: Managing your own equipment grants you the freedom to choose and customise technologies, select providers, and support the tools that best meet your community's needs.

Privacy: Knowing exactly who has access to the data, understanding the processes in place and documenting everything allows for enhanced privacy for all users of the space.

Politics: The politics of communal infrastructure often align with free/libre and open source software (FLOSS) principles, emphasising transparency, collaboration and community empowerment.

Security: By selecting, installing and managing the infrastructure, you can enforce stricter access controls and better protect your resources from external threats.

Agency: Designing and operating your own infrastructure gives you the ability to make informed choices, understand your limitations, and make changes when necessary. It also instils confidence in your community's ability to manage various challenges and situations.

In essence, communal infrastructure isn't just about technology; it's about empowering people to take control of their digital lives, ensuring that their online interactions are secure and private and that no outside entities can access their stored data or control their communication channels.

COMPONENTS OF COMMUNAL INTERNET INFRASTRUCTURE

There is no single model for communal infrastructure deployments: they vary in structure, size and administration model. In this section we will describe the different components of communal infrastructure and some of its models.

PEOPLE

In communal infrastructure, there is often a significant overlap between users, decision-makers (managers), and technical staff. Ideally, everyone involved in such deployments would have the opportunity to participate at all levels if they want. However, due to the complexity of modern internet systems, specialized roles are necessary.

For example, the technicalities of setting up and maintaining a self-managed internet server infrastructure require a team with diverse skills and expertise to ensure the system is designed and operated with people as its centre, and that the implemented applications are robust, secure and reliable. Here's an overview of the key roles typically involved:

Curators are the people who facilitate online spaces, organise online content, create and manage user accounts, etc.

Depending on the specific implementations, technologies and services, you will need other roles like **network engineers, security specialists, database administrators (DBAs), front-end/back-end web developers, web designers, cloud/ infrastructure architects**, etc.

System administrators are responsible for installing, configuring and maintaining the server hardware and operating systems. They manage user accounts, monitor system performance, and ensure the servers are running smoothly.

Support/help desk staff provide technical assistance to users and troubleshoot any issues that arise with the infrastructure. They can also write support manuals and conduct trainings.

Each of these roles contributes to the overall stability, security and efficiency of a self-managed internet infrastructure. Depending on the scale, scope and complexity of the infrastructure, some roles might overlap or be combined, or some can be provided by external staff, but having a team with these core competencies is essential for successful operation and maintenance. In a solution designed with people as its centre, it is important to consider that there should be mechanisms for users to participate and learn to perform more specific tasks if they so wish – so they can further expand their ownership of the platform.

HARDWARE MODELS

In a virtual world, the physical hardware that supports our online activities – computers, servers, devices, antennas, cables – often feels distant and abstract. However, every time we access an online resource, we rely on hundreds of these tangible elements. While some of this hardware may be under our control, much of it is not, and this can significantly impact our privacy and security. In this section we will discuss four server hardware models that offer different levels of control.

FULL OWNERSHIP AND CO-LOCATION OF A "BARE-METAL"

You have maximum control when you have your own physical servers and co-locate them with an ISP or in a data centre you trust. In this setup, the ISP/data centre provides essential services such as electricity, internet connectivity and fail-safe mechanisms, while also ensuring the physical security of your server. In this scenario, you are responsible for purchasing your hardware, installing it in the data centre, connecting wires, and replacing the hardware if it fails.

Considerations: When choosing an ISP or data centre for co-location, factors like the country of its location are crucial. This choice affects the legal framework you are subject to, including data privacy laws and compliance requirements. However, owning and managing your own server at this level requires significant technical expertise, often referred to as managing "bare metal" servers. This capability can also be costly, making it less accessible for many individuals or small communities. In many cases, it entails someone being able to access the place where the server is located to undertake the physical maintenance, although in some other cases you may rely on your co-location provider to perform simple operations like manual restarts or changing wires.

FULL VIRTUAL SERVER (VIRTUAL ACCESS TO A BARE METAL)

If you don't want to bother with hardware repairs but want full control, you can purchase/rent an entire virtual server. Here, your provider is responsible for the hardware maintenance of the bare metal. You are granted virtual access to the machine and are fully responsible of the installation, starting from choosing and remotely installing the operating system, deploying virtualisation and automation, configuring networking, and installing the desired software. This option allows you to run on the same server several virtual machines for different services or for different partners.

Should you face a hardware failure or issue, you need to inform your provider and request the replacement, and you rely on them for any upgrades or technical issue-solving.

OWNING PART OF A SERVER (VIRTUAL MACHINE MODEL)

A more common and cost-efficient model is to own a part of a server through a virtual machine (VM). In this scenario, you don't have direct access to the server's hardware or low-level operating system, but instead operate within a separate virtual instance that you can fully configure and control.

Practicality: This model strikes a balance between control and practicality. It allows for customisation and management of the operating system and networking setup within the VM, giving you control over most aspects of the server's operation. However, since you are sharing the physical server with others, you may have less control over the hardware itself and there may be limitations for further virtualisations (you may experience obstacles to deploy containers or nested VMs within your VM).

Maintenance and expertise: Administering a server, whether it's a full server or a virtual instance, requires ongoing maintenance. This includes keeping the operating system updated, protecting the server from cyberattacks, maintaining backups and regularly monitoring logs. These tasks demand time, resources and technical expertise, which can be a challenge for some communal infrastructure models.

SHARED WEB HOSTING

If you only need a website and no other services, you may be interested in shared web-hosting providers. Here, you are only granted some space within a web server managed by your provider. **Cons**: You have very little control over the security setup; and if you need any special plugins or features, you have to request your provider. **Pros**: You need only minimal tech savviness, and often there are a lot of different offers for "one-click" deployments of popular software; so it is often a very economical option.

SUMMARY OF RESPONSIBILITY AND FEATURES

	BARE METAL	FULL VIRTUAL SERVER	VIRTUAL MACHINE	SHARED HOSTING
HARDWARE	YOU	PROVIDER	PROVIDER	PROVIDER
OPERATING SYSTEM	YOU	YOU	YOU	PROVIDER
FURTHER VIRTUALISATION	YES	YES	NO OR VERY LIMITED	NO
BACKUPS	YOU	YOU	YOU AND/OR PROVIDER	PROVIDER
SECURITY	YOU	YOU	YOU AND PROVIDER	PROVIDER
SOFTWARE CHOICE	FULL	FULL	MORE OR LESS YOURS, ALTHOUGH WITH CERTAIN LIMITATIONS	VERY LIMITED

BALANCING CONTROL, COST AND EXPERTISE

For communal internet infrastructure, the choice of hardware and server setup is a critical decision that balances control, cost and the level of technical expertise available within the community. While full server ownership offers the highest degree of control, it also comes with higher costs and requires substantial technical knowledge. Virtual machine models offer a more accessible option, providing significant control while being more affordable and easier to manage.

Ultimately, the level of control you have over your hardware will directly impact the privacy and security of your online activities. In communal infrastructure models, these decisions can be made collectively and transparently, taking into account the community's needs, resources and technical capabilities.

SOFTWARE

The software that needs to be installed on a server (called a “stack”) is largely determined by the services you want to offer. At its foundation, the stack always includes the operating system and its related applications, forming the base upon which all other software runs.

When selecting applications to install, several key factors should be carefully considered:

Support models: Consider whether the software comes with reliable support, either through community forums, vendor support contracts, or third-party services that you can trust. Reliable support can be essential for customising, troubleshooting and maintaining the services operational (uptime).

Licensing type: Understanding licensing agreements is crucial, especially in terms of cost, usage rights and compliance. Open source licences, for example, can offer flexibility, privacy and community support, while proprietary licences might provide more specialised features and vendor support.

Technical expertise: It is important to choose software that aligns with the skills and knowledge of your technical staff. If the team is already familiar with certain platforms, it can significantly reduce setup time and improve operational efficiency.

Accessibility and adaptability: Take into account whether the software provides easy language customisation and adaptation for diverse user capacities and contexts. For example, do you need to always have an excellent internet connection to use the system, or is it also adapted to usage with slow internet access?

Ecological impact: Consider whether the software was developed with energy efficiency in mind and optimised to reduce CPU, memory and network bandwidth usage.

Ease of use: The software should be straightforward to operate, for the user community, for administrators and for the technical team. This is especially important if your technical team and administrators have varying levels of expertise. Simpler, more widely adopted tools can reduce the learning curve and operational errors. While modern and friendly user interfaces encourage more users to adopt platforms that may seem unfamiliar.

Regardless of the solutions you implement, the most critical aspect of software management is ensuring that applications are always kept up to date. This includes regularly applying security patches and updates as soon as they are available. Timely updates are vital for protecting your infrastructure from vulnerabilities and ensuring the stability and security of your services.

CONNECTIVITY

When data travels across the internet, it passes through a complex web of networking components owned by various entities such as internet service providers (ISPs), government networks, internet exchange points (IXPs) and private sector infrastructure. Each of these entities plays a role in the transmission of your data, but they also introduce layers of control and regulation.

In most cases, when you host your server(s) with an ISP/data centre, you are dependent on their networking infrastructure and connectivity. This means you'll also have to comply with their specific guidelines and the local/national legislation governing their operations, as well as comply with required regulations. This is why it's crucial to choose a provider that aligns with your values, particularly regarding data privacy, access rights and overall security.

If you require enhanced protection for the data stored on your server, or the data originating from and travelling through it, you should consider implementing security measures such as server encryption, virtual private networks (VPNs), and secure tunnels for data transit. These tools help safeguard data both at rest (while stored) and in transit (while being transmitted), ensuring that sensitive information remains protected from unauthorised access.

Though in most cases you will rely on a data centre to host your servers, in some cases, community networks offer an alternative model where the "last mile" infrastructure – the final leg of the data journey to the end-user – is managed by the community itself. In some implementations, this can also include data centres managed by the same community. This approach provides greater control over connectivity, fostering a network that reflects the community's values and priorities regarding privacy, accessibility and security. For more insights into community networks and how they function, you can explore a wide range of articles and publications on the subject at apc.org.

SERVICES OF COMMUNAL INFRASTRUCTURE

Communal infrastructure can take many forms, with services tailored to the unique needs of the community it serves. These services are designed with a focus on privacy, security, accessibility, and the promotion of community values. Here are some examples:

Email Services: Providing secure and private email services is a key component of many communal infrastructures. Unlike mainstream email providers, these services are designed to guarantee privacy and data protection, ensuring that user communications are not subject to surveillance, data mining or advertising.

Website design and hosting: Communities can offer website design and hosting services that prioritise data privacy, security and autonomy. These services allow individuals and organisations within the community to create and maintain their online presence without relying on commercial hosting providers which may have different priorities or impose restrictive terms of service.

Online Conferencing Systems: Secure, community-hosted online conferencing platforms, such as those based on Free/ Libre and Open Source Software (FLOSS) like BigBlueButton (BBB), enable safe and private virtual meetings. These systems ensure that communication is encrypted, and that user data, meeting information and recordings are not harvested or shared with third parties.

Solutions for Online Work: Real-time collaboration tools, such as shared document editors, project management systems and chat platforms, are essential for facilitating online work within a community. These tools are developed and managed in a way that respects user privacy, encourages open participation and supports the community's workflow. Curators play a critical role in maintaining online spaces active and updated.

Data Storage Services: Community-managed data storage services provide a secure and private alternative to commercial cloud storage providers. These services ensure that data is stored locally or within a trusted network, giving users control over who has access to their information and how it is used. The server's location jurisdiction can be critical in guaranteeing the level of government access to the hosted data.

Internet Access Services: Community networks can be a vital component of communal infrastructure, particularly in areas where traditional ISPs are not available or affordable. These networks offer "last-mile" connectivity, managed and operated by the community itself. They can provide reliable, low-cost internet access while promoting digital inclusion and local empowerment.

These services not only enhance the community's ability to communicate and collaborate but also align with the principles of autonomy, privacy and collective ownership. They represent a shift away from the centralised, corporate-controlled internet infrastructure towards a model that is more democratic, transparent and responsive to the needs of the community.

GUIDING PRINCIPLES OF GOOD COMMUNAL INFRASTRUCTURE DESIGN AND OPERATION

There are hundreds of different ways to actually implement communal internet infrastructure concepts in the form of real world infrastructure.

We must always remember that we are referring to infrastructure that is built for people and by people. Clear co-management organisational models with sustained social praxis are an essential component for the success of these solutions. However, they require time and effort, and are difficult to sustain over time – unfortunately, this is where community/shared/communal infrastructures may also break down.

In this section, we present a few concepts that need to be considered when designing and operating good communal infrastructure.

Participation

Communal infrastructure is built with the needs of the community in mind. Depending on the community, builders and maintainers of the technical infrastructure and the community of users may not share all the same perspectives. Therefore, it is key that participatory models are used when designing, implementing and operating the systems and services.

Written documentation

In every project of this type there are many agreements that are not always well established, verbalised and made visible, accountable and (re)negotiable. It is a good idea to have written agreements about everything possible. For example, organising the work around the needed systems requires formally agreed on policies and clearly defined procedures. That way, there is transparency and clarity to manage the daily work. Remember that all documents should be live documents that change as the organisation, needs, services and reality change.

Openness

Make sure people can move out of your systems easily if they so wish, and move into your systems when they want, ensuring data portability, open standards and clear user guidelines.

Security

Unfortunately, it takes a lot of resources to maintain servers and information online, as attacks are becoming more frequent. Guaranteeing the security of the installations, platforms, tools and spaces must be a priority.

User support

We need to help people make the best use of the infrastructure. User support can include capacity building tools in a variety of formats, like live sessions, recorded trainings, online courses and videos, and instruction manuals. These have to be designed taking into account the specificity of our users, their language preferences and their content delivery preferences (text, audio, video, etc.). In cases of larger implementations, user support can also include a help desk service, email support and even remote assistance.

SUSTAINABILITY

Sustainability for self-managed internet infrastructure involves several dimensions, each addressing a critical aspect for long-term viability.

Below are the key types of sustainability to consider:

Community/operational sustainability is about ability of the community to continue managing and running the infrastructure effectively. It includes activities like building local technical capacity through training and education, fostering a strong sense of ownership among community members, establishing governance structures for internal decision making and transparent management, and encouraging participation and contributions from a broad user base. Governance models for communal infrastructure can vary widely, from those that lean toward a service-oriented model to some that are far more fluid and distributed, it's important to keep in mind the desires, capacity and incentives for participation when choosing a model for the community.

Social sustainability is about ensuring that the infrastructure serves the social and cultural needs of the community in an inclusive and equitable way. It implies ensuring access for all community members, especially marginalised groups and minorities, but also protecting users' privacy and fostering trust within the online spaces. It can also include tailoring the technologies and applications to reflect and respect local cultures, languages and values. It also encompasses encouraging gender inclusivity and other social equity considerations, like making sure your tools are usable and accessible for everyone.

Technical sustainability includes making sure that the infrastructure continues to function over time without frequent breakdowns or failures, and with excellent uptime. It includes regular maintenance of hardware and software, updating systems, doing backups to protect against data loss, and planning adequate scalability to accommodate growing needs. It also must contemplate having technically qualified people capable of running the infrastructure efficiently.

Economic/financial sustainability is about the ability to generate or secure financial resources to maintain the infrastructure working over time. This includes developing business models (e.g. subscription fees, cooperative models) and mechanisms to secure funding through generating sources of income, donations, grants or community contributions. But it can also include minimising costs by leveraging open source technologies and hiring community-driven expertise.

Environmental sustainability refers to minimising the ecological impact of the infrastructure and aligning it with sustainable environmental practices. This can be achieved by using energy-efficient hardware and renewable energy sources, minimising e-waste and ensuring responsible disposal of outdated equipment, reusing or recycling materials where possible, optimizing processor use and data transit, and reducing carbon footprints by avoiding energy-intensive data centres. If you hire hosting providers, try to make sure that they are aligned with these practices as well. Maintaining good online hygiene also helps: regularly clean up content, minimise data stored online, reduce data transfers and have a clear data retention policy.

Institutional/legal sustainability is about ensuring that the infrastructure operates within the corresponding legal and policy framework. It includes ensuring compliance with local, national and international laws, as well as data protection and other relevant regulations according to the applicable jurisdiction(s). But it can also include developing partnerships with local institutions, cooperatives or municipal bodies to foster long-term support and establishing legal protections for community ownership and management

Cultural and ethical sustainability has to do with aligning the infrastructure with the ethical principles and cultural practices of the community it serves. It can include tasks like ensuring the system promotes the ethical use of the internet (e.g. open access, privacy, freedom of expression), preserving and promoting local cultural practices, languages and traditions, and encouraging a values-based approach to the technology (e.g. feminist principles, solidarity economies).

Political sustainability refers to the capacity to navigate and influence political environments to maintain the self-managed infrastructure. Some of its key elements include building alliances with similar-minded projects and organisations, advocating for policies that promote community-managed infrastructure and digital sovereignty, offering safe spaces in the face of political challenges like internet shutdowns, censorship or restrictive policies, and ensuring community control and autonomy in decision-making processes.

By considering these various forms of sustainability, communities can create resilient, self-managed internet infrastructures that thrive in the long term and serve the collective interests of their members.

THE FUTURE OF COMMUNAL INTERNET INFRASTRUCTURE

We hope that this introductory paper has provided you with interesting food for thought on the underlying politics of designing and implementing communal infrastructure services.

We believe that the future of communal internet infrastructure looks promising, as more and more deployments take these human-centred values into account when operating online services. As more communities share their success stories and models, the knowledge and expertise required to build and sustain these services will become more widespread, encouraging others to adopt similar approaches.

Once again, we would like to thank the participants in the session on community infrastructure at APC's Community Gathering 2024, who provided valuable inputs and ideas for us to produce this document.

We will further update this paper as we gather more insights into specific deployments of communal infrastructure models from APC members and partners.

USEFUL REFERENCES

APC's Local Access Networks project
https://www.apc.org/en/project/local-access-networks-can-unconnected-connect-themselves

"The politics and practices of an autonomous technology: Voices of the members of May First"
https://mayfirst.coop/files/politics-practices-autonomous-technology.pdf

"Best practices: Diversity and inclusion in open source projects"
https://www.apc.org/en/pubs/best-practices-diversity-and-inclusion-open-source-projects

"Community networks and feminist infrastructure: Reclaiming local knowledge and technologies beyond connectivity solutions"
https://www.genderit.org/feminist-talk/community-networks-and-

"Feminist infrastructure: The creation of what sustains us"
https://genderit.org/feminist-talk/feminist-infrastructure-creation-what-sustains-us

APC's Closer Than Ever documentation
https://www.apc.org/en/publications/closer-than-ever