THE LINUX FOUNDATION | Research

Standing Together on Shared Challenges

Report on the 2023 Open Source Congress

Anthony Williams, President and co-founder, *DEEP Centre*
Foreword by Yue Chen and Chris Xie, *Futurewei Technologies, Inc*

December 2023

Sponsored by
FUTUREWEI Technologies

Standing Together on Shared Challenges

As a collective knowledge base for humanity, **open source thrives on core principles** such as transparency, inclusivity, and community-driven development.

Maintaining the resilience of open source requires a community-wide commitment to addressing shared challenges such as cybersecurity, artificial intelligence (AI), and techno-nationalism.

The security of open source software (OSS) depends on a **healthy talent pool of cybersecurity professionals** and an incentive structure to attract and retain maintainers.

The open source community should embrace a **"security by default"** model, with security at the foundation of application design.

Rising OSS adoption has increased regulatory scrutiny, making policy advocacy and education critical to ensuring new regulations are compatible with open source principles and practices.

Open source foundations must harness their legal acumen, communication, and community engagement skills to **advocate effectively in the policy arena.**

Digital sovereignty measures can increase fragmentation and impede regulatory harmonization, but national efforts to promote technological autonomy have also led to greater open source adoption.

Foundations can mitigate geopolitical tensions by establishing neutral protocols for managing community contributions and maintaining the flow of knowledge and technology across borders.

The community can attract new talent and maximize its social impact by **committing to diversity and inclusion** and using codes of conduct to promote shared norms.

Explainability and provenance are crucial to increasing the trustworthiness of AI systems and addressing licensing, security, and governance concerns.

Transparency and openness are central to managing the new risks and ethical considerations associated with increasingly powerful and pervasive AI systems.

Models for greater collaboration include a new global secretariat to steward open source or a peer-to-peer network of OSS community leaders.

Contents

Foreword 4

Introduction 5

An era of unprecedented challenges for the open source community 5

The 2023 Open Source Congress in Geneva 6

Deciphering Open Source Security 8

Open source security needs a new paradigm for working with the maintainer community 8

The OSS ecosystem must help build the talent pool for addressing security challenges 9

Security by default should be a priority for the OSS community 10

The Impact of Technology Policy for Decentralized Organizations: Challenges and Opportunities 11

The growing ubiquity of OSS has made regulation an inevitability 11

Policy advocacy and education are critical to the continued success of the open source ecosystem 12

Effective policy work requires specialized skills and increased collaboration between OSS foundations 13

Keeping Collaboration Global, Open, and Inclusive: Examining the Impact of Export Controls, Digital Sovereignty, and DEI 14

Digital sovereignty poses opportunities and challenges for open source 14

Techno-nationalist policies are causing some fracturing and siloing in open source communities 15

Diversity and inclusion are an essential part of the landscape and conversation about open collaboration 17

Does AI Change Everything? What Is Open? Liability, Ethics, Values 18

Openness in AI entails more than just access to the source code 18

AI-generated code will create challenges in open source licensing, security, and regulation 19

Systemic risks from AI require an urgent, open source response 20

The Imperative for Open Source Collaboration 23

Identifying shared priorities for the open source ecosystem. 23

Creating a structure and process for effective collaboration . 24

Conclusion 26

Acknowledgements 27

About the author 27

References 28

Foreword

In the rapidly evolving digital age, open source as a collective knowledge base for humanity stands as a beacon of hope and progress. Rooted in core principles of transparency, inclusivity, and community-driven development, open source represents a collaborative endeavor that transcends borders and cultures. As we gather insights from the 2023 Open Source Congress, it becomes evident that the strength of open source lies not just in its code but in the global community that nurtures it.

The resilience of open source is a testament to our shared commitment. As we navigate the complexities of cybersecurity, artificial intelligence (AI), and the emergence of techno-nationalism, it is imperative to ensure the security of open source software (OSS). Security, a paramount concern in our interconnected world, demands more than sporadic fixes and patches. True open source security necessitates a systematic and holistic approach, addressing the symptoms and the root causes of vulnerabilities. It is an urgent call to action for open source infrastructure service providers and practitioners to champion the principle of "security by default." Easily accessible security tools, robust standards, protocols, and best practices can empower developers to fortify their creations from the ground up.

The growing adoption of OSS places it at an important juncture, facing heightened regulatory examination. The increased regulatory scrutiny necessitates a proactive approach to policy advocacy and education. Ill-informed regulations threaten to undermine the foundational values of open source. Such measures, resulting from a lack of understanding of the nature of open source, risk stifling innovation, erecting barriers to collaboration, and fragmenting the global open source communities. Open source foundations, equipped with legal expertise, communication prowess, and community engagement, are in a unique position to advocate in the policy arena, ensuring that regulations are compatible with open source principles.

As AI continues to permeate every facet of our lives, the principles of open source become even more crucial. Openness and transparency are central to addressing the challenges of AI safety. By adopting open source principles in AI development, AI systems will be powerful as well as ethical, accountable, and secure.

Looking to the future, diversity, inclusion, and shared norms will continue to serve as the cornerstone for open source growth and impact. Whether through a global secretariat or a peer-to-peer network, models for a united front for the global open source communities will help ensure that open source remains a collective knowledge base for humanity. Our hope is that we will stand together, ready to address our shared challenges and shape a brighter, more open future.

Together in open source,

Yue Chen, Head of Technology Strategy
Chris Xie, Head of Open Source Strategy
Futurewei Technologies, Inc.

Introduction

Since the 1980s, open source has grown from a grassroots movement to a vital driver of technological and societal innovation. The idea of making software source code freely available for anyone to view, modify, and distribute comprehensively transformed the global software industry. But it also served as a powerful new model for collaboration and innovation in other domains.

By the turn of the century, a shared approach to software development had spawned large-scale collaborative efforts around open standards, open hardware, and open data.[1] As a result, there is hardly a digital tool or application in use today that does not embody open source code or whose developers have not been profoundly influenced by open source methods.

The principles of transparency, inclusivity, and community-driven development continue to shape how we innovate, share knowledge, and solve complex problems in the digital age. Beyond the world of technology and software development, open collaboration is catalyzing profound institutional transformations, including the rise of open government, open science, and open education. The collaborative, transparent, and cost-effective nature of open source software (OSS) has also made it indispensable to global efforts to address climate change and cure intractable diseases, among other issues.

An era of unprecedented challenges for the open source community

After decades of sustained progress, the open source community today is facing an era of unprecedented challenges. For example, while powerful open source approaches can spark groundbreaking advancements, they are also open to exploitation by nefarious actors. Just as proprietary software products can be compromised by bad actors, open source's very openness has made it vulnerable to exploitation by cyber criminals and other actors, who have introduced vulnerabilities and backdoors into open source projects. Sophisticated OSS supply chain attacks are increasing and have alerted the OSS community to the urgent need to bolster its cybersecurity posture.[2]

At the same time, the growing ubiquity of OSS has intensified regulatory scrutiny. In the past two years alone, the CISA Open Source Security Roadmap[3] in the United States and the European Union's Product Liability Directive and Cyber Resilience Act (CRA) have introduced measures to increase liability for product safety and require more timely disclosure and patching of security vulnerabilities.

Unfortunately, some of these otherwise well-intentioned regulatory initiatives lack a nuanced understanding of the implications for the open source community's unique development, commercialization, and licensing models. As a result, they pose significant compliance challenges. Some argue that new regulations could break the open source development model that gave rise to Linux, the Apache web server, Mozilla Firefox, and many other seminal pieces of foundational digital infrastructure. As regulatory challenges accumulate, OSS foundations are being called upon to help developers comply with new regulations and to engage earlier and more assertively in shaping new legislation in the digital arena.

Open source has thrived because of the community's steadfast commitment to openness, collaboration, and the unfettered flow of information across borders. Here, too, the community is confronting new barriers to cross-border cooperation. Global trade tensions, geopolitical conflicts, and a heightened emphasis on digital sovereignty have emerged as genuine impediments to international collaboration on digital technologies. For example, a surge in so-called techno-nationalism has prompted countries including the United States and China to introduce strict export controls on semiconductors and a range of other critical technologies. Many in the open source community worry that curtailing trade in technology could lead to the fragmentation of OSS development into regional enclaves, thwarting efforts to promote inclusivity and cultivate a more diverse talent pool within the community.

Finally, the accelerating deployment of artificial intelligence systems in software development also poses difficulties for the OSS community. AI-enabled code generators can turn a natural language prompt into a fully coded function in a matter of seconds. The potential benefits to productivity in the software industry and beyond are undeniable. However, the uncertain provenance associated with the code generated by AI models could lead to the inadvertent misuse of proprietary or licensed code, leading to potential infringement issues and other concerns related to licensing and cybersecurity.

More broadly, today's massive investments in AI promise rapid advancements, including groundbreaking applications in healthcare, transportation, public administration, finance, and education. At the same time, the growing influence of AI has given rise to new risks and ethical considerations related to bias, transparency, privacy, job displacement, and longer-term threats to humanity. Companies racing to deploy and monetize a new generation of AI technologies have mainly insisted on secrecy and proprietary development models. Meanwhile, the open source community is seeking to prove that a genuinely open approach to AI provides a better pathway for ensuring that AI systems align with human values, safeguard human rights, and promote society's overall well-being.

The 2023 Open Source Congress in Geneva

The influence of open source today is global, and with worldwide reach and impact comes a profound responsibility. Regulation, techno-nationalism, AI, and cybersecurity are transforming the open source landscape and creating an imperative for collective action. Many stakeholders in the open source community recognize that greater collaboration among OSS projects and the foundations that support them is urgently needed to enable community members to stand together on these common challenges.

OSS foundations have different mandates, constituencies, and roles in the ecosystem. In the past, differing philosophical orientations and perspectives have impeded collaboration. However, in light of the shared challenges, leaders from across the global OSS community recently set these differences aside and forged new alliances to ensure the continued success of the ecosystem.

In July 2023, 53 open source leaders representing 37 organizations came together in Geneva, Switzerland, for the Open Source Congress. The mandate for the Congress was to identify shared values, build relationships among key stakeholders, and devise a plan for sustaining the vibrancy, resilience, and integrity of open source.

Selecting Geneva as the venue for the Congress was symbolic. The birthplace of the famed Geneva Convention, Geneva has long been a neutral ground, a place for nations to resolve their disagreements and find commonality. The leaders of sovereign nations have frequently gathered in Geneva to frame the rules of engagement that guide international relations—efforts grounded in a shared commitment to advancing the welfare of humanity.

In a similar spirit, open source leaders attending the Congress were asked to rise above regional divides, ideological differences, and the contemporary geopolitical climate. Attendees broadly recognize that open source is a collective good that transcends borders and depends on international collaboration and effective ecosystem governance. The challenge to open source leaders was to forge a mutual commitment and action plan for ensuring fidelity to the community's essential principles of openness, inclusivity, and community-driven development.

More concretely, Congress participants in Geneva were tasked with the following objectives:

- **To examine and discuss critical challenges** facing the open source community
- **To explore pathways** for enhancing inter-foundational collaboration, including mechanisms to uphold shared values and strategies for addressing common challenges
- **To establish new channels** for follow-up discussions and sustain momentum on specific actions required to support any agreements forged in Geneva

Attendees broadly recognize that open source is a collective good that transcends borders and depends on international collaboration and effective ecosystem governance.

On the morning of July 27, 2023, Congress participants engaged in a series of panel discussions organized around four pressing challenges for the open source community:

- **Deciphering open source security:** a discussion focused on promoting trust and confidence in OSS solutions by addressing security vulnerabilities and maintaining critical OSS infrastructure
- **The impact of technology policy for decentralized organizations:** a roundtable on building coordinated responses to embrace emerging regulatory initiatives that could affect OSS development and deployment
- **Keeping collaboration global, open, and inclusive:** a critical look at the geopolitical barriers to collaboration, including export controls and digital sovereignty initiatives related to data, semiconductors and other essential technologies
- **Does AI change everything:** an examination of the potential risks AI poses to the OSS ecosystem, including license violations, copyright infringement, human capital, and social good

In the afternoon, the focus turned to bringing key stakeholders together to address the open source community's most urgent challenges. Congress participants explored various mechanisms for enhancing collaboration, including options such as forming a new global secretariat for the open source community and creating a lightweight peer-to-peer network to coordinate the efforts of OSS foundations. The discussions in Geneva concluded with a resounding consensus that there is tremendous value in regularly convening leaders of OSS foundations and working collectively to steward the global open source ecosystem. The remainder of this report documents the proceedings of the 2023 Open Source Congress and highlights key discussion points and conclusions from this momentous day.

Deciphering Open Source Security

Like other categories of software, OSS is not immune to security vulnerabilities. Flaws can exist in the code, and when discovered, they can be exploited by malicious actors. These vulnerabilities may result from coding errors, lack of updates, or insufficient security reviews. Attackers have recently targeted the software supply chain, injecting malicious code into open source libraries and components that are widely used. These attacks can compromise numerous applications that rely on these libraries, triggering potentially catastrophic failures and breaches for organizations that rely on OSS.

Given the stakes, it's no surprise that the first panel of the day brought together open source community leaders to discuss the critical issues surrounding the security of OSS and strategies to enhance its resilience. Securing and safeguarding critical open source infrastructure has become a focal point for collaboration in the OSS ecosystem. Congress participants started from the assumption that building trust and confidence in OSS and supporting the ongoing maintenance of critical open source infrastructure are urgent imperatives. The key questions for debate revolved around how best to organize the OSS community to accomplish these objectives.

Open source security needs a new paradigm for working with the maintainer community

Decentralized innovation is producing a remarkable tapestry of open source components that are being widely deployed to support the digital economy. As Congress participants explained, these components are embedded in numerous pieces of critical infrastructure that provide the underpinnings for global commerce, from power grids, shipping, and transportation to electronic commerce and finance. Understanding which components are most widely used and most vulnerable to exploitation is crucial for the continued health of the open source ecosystem and the broader digital economy. Doing so is also, as one participant noted, essential to providing a secure infrastructure for everyday Internet users.

Open source leaders in Geneva observed that maintaining the disparate OSS components in use today is a complex challenge that requires a transparent and coordinated approach and a more significant deployment of funding and resources from the principal beneficiaries of open source infrastructure. More specifically, Congress participants pointed to several interrelated challenges.

One challenge is tracking the proliferation of OSS and monitoring potential vulnerabilities. With hundreds of thousands of OSS packages in production applications throughout the supply chain, understanding precisely which OSS components are most widely used is a non-trivial task. When security incidents arise, the absence of central authority to ensure quality and maintenance makes it challenging to organize a coordinated disclosure of potential vulnerabilities and assign responsibility for correcting the problems. The open source ecosystem needs to be able to apply common processes and unified best practices.

A second challenge is maintaining the vast number of critical OSS components in use today. Congress participants noted that in most cases, there are no official resource allocations and few formal requirements or standards for maintaining the security of critical open source code. While high-profile projects, such as Linux, have active communities and receive regular attention, other projects are infrequently updated and have few watchers.

Several participants suggested compensating maintainers to focus on security, especially those who may otherwise lack the time and resources to perform regular updates and maintenance. Compensation needn't always entail committing additional financial resources. OSS projects such as EleutherAI have incentivized contributions and maintenance activities by adding significant contributors' names to the citation data for major code libraries and academic research papers.

Congress participants also welcomed the efforts of the Open Source Security Foundation (OpenSSF), which became a funded project in 2021. The OpenSSF plays a vital role in coordinating efforts to secure OSS between the public sector, the private sector, and the community. A critical function will be directing resources to unsupported or under-resourced areas. Given the scale of the task, Congress participants called for more sustainable funding sources to address security vulnerabilities at source and at scale.

Despite these challenges, Congress participants were keen to point out that OSS is not inherently less secure than proprietary software. In fact, open source can offer advantages for security, such as transparency (allowing anyone to review the code), rapid responses from the community when vulnerabilities are discovered, and the ability to customize and harden software for specific security needs.

> *The proliferation of cyberattacks and data breaches across all digitally enabled products and services has raised awareness of the importance of cybersecurity.*

The OSS ecosystem must help build the talent pool for addressing security challenges

As noted, many open source projects operate with limited resources, including funding and personnel. The lack of people power can affect the ability of projects to conduct security audits, respond to vulnerabilities, or provide timely support. However, Congress participants pointed to another related systemic challenge: an industry-wide scarcity of cybersecurity professionals.

The proliferation of cyberattacks and data breaches across all digitally enabled products and services has raised awareness of the importance of cybersecurity. As threats become more sophisticated, the demand for skilled professionals to defend against them has grown significantly. Moreover, with the growth of cloud computing, the Internet of Things, and mobile devices, the attack surface has expanded considerably, creating new challenges for securing systems and data. Cybersecurity is also a broad field with various specializations, including network security, application security, penetration testing, incident response, and regulatory compliance. Large enterprises are struggling to find professionals with the right specializations in an increasingly competitive global market for talent, which makes the challenge for open source projects even starker.

In light of these challenges, Congress participants posed a series of questions for the OSS community to consider. What tools and training can we give the community to make faster progress on security? Can we redefine what it means to be a security professional? Can we increase diversity in our developer base, thereby attracting new talent to the ecosystem? Can we contribute to increasing the focus on cybersecurity in computer science programs?

Potential solutions to the cybersecurity talent crunch could include cybersecurity training programs and certification courses, partnerships with colleges and universities to create updated cybersecurity curriculums, and DEI initiatives to help fill the talent gap. Congress participants agreed that OSS foundations should pursue further discussions and action on these priorities.

Finally, in a related observation, Congress participants noted that a lot of small businesses depend on OSS but have limited in-house resources for managing IT security. One participant estimated that 95% of small businesses have no people to manage software security. The lack of resources to manage IT security makes the small business community particularly dependent on the OSS community for timely support.

> *Security by default entails designing and developing software applications with security as a primary consideration from the outset and making security the default state rather than an afterthought.*

Security by default should be a priority for the OSS community

In closing the discussions on cybersecurity, Congress participants talked about the need for the OSS community to move toward a “security by default” model. Security by default entails designing and developing software applications with security as a primary consideration from the outset and making security the default state rather than an afterthought. According to open source security leaders assembled in Geneva, key steps include defining security requirements early in the software design phase, performing regular security reviews in the production phase, and automating security testing, patching, and compliance auditing once the software is in deployment.

Congress participants agreed that a security by default model and automating security testing and maintenance processes would significantly reduce the likelihood of security breaches and vulnerabilities in OSS applications. It would also free up developers and maintainers for other critical tasks in the ecosystem. As one participant put it, “The more we can create security by default, the more we can focus on higher-order problems.”

The Impact of Technology Policy for Decentralized Organizations: Challenges and Opportunities

The discussions surrounding cybersecurity highlighted why good governance and policy engagement are increasingly paramount to the ongoing success and resilience of the OSS ecosystem. However, beyond cybersecurity, there are many other Internet policy issues that pose significant challenges and opportunities for users and developers of open source solutions. For example, in critical matters such as intellectual property, privacy, product liability, and antitrust, there is a widely shared view that the open source community has not been as influential or assertive in technology policy dialogues as it should, resulting in regulatory initiatives that put the open source model at risk. At the same time, OSS offers solutions addressing many of the pivotal policy challenges of our time. Yet, the community's lack of visibility in policy circles means the community's socio-economic contributions are often underappreciated.

As open source leaders gathered in Geneva, discussions naturally turned to the consequences of recent regulatory actions on the open source ecosystem, the need to educate the global policy community about OSS's unique characteristics and methodologies, and the imperative for OSS foundations to prioritize increased collaboration and capacity-building for effective policy engagement and advocacy.

The growing ubiquity of OSS has made regulation an inevitability

Open source software has become a fundamental and pervasive element of today's technology landscape. Its influence continues to grow as it underpins innovations across various domains, fosters collaboration among developers and organizations, and democratizes access to powerful software tools and solutions. By some estimates, open source components power 70 to 90% of modern software solutions, including applications ranging from web development and machine learning to cloud computing, data science, and scientific research.[4]

With the growing ubiquity of OSS has come increased regulatory scrutiny. For example, the dominance of the Linux operating system in the server and cloud computing market has raised concerns about competition and antitrust issues. Data privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe, have focused attention on whether OSS packages for data processing and storage comply with data protection laws. In the wake of Log4Shell, regulators are investigating whether organizations are properly managing open source components and addressing security vulnerabilities. More broadly, concerns about cybersecurity and critical infrastructure have led to assessments of the role of open source solutions in national and corporate cybersecurity strategies.

Congress participants described Europe as a vital "battleground" for technology policy, noting that the E.U. is often a first-mover in technology policy while the United States tends to take a wait-and-see approach. Indeed, European regulators have moved faster than any other jurisdiction to safeguard data privacy, promote competition, ensure cybersecurity, and address the socio-economic challenges posed by emerging technologies. In the last five years alone, Europe has introduced the GDPR to establish standards for data protection and privacy, the Digital Markets Act to regulate large digital platforms and prevent anti-competitive practices, the Digital Services Act to combat illegal content and enhance transparency in online services, and the AI

Act to govern the development and use of AI. Most recently, the E.U. proposed the CRA to bolster the cybersecurity requirements for products with digital elements and updated its Product Liability Directive for the digital age.

The critique of European technology policy—and regulators in legislative processes, despite the critical role that OSS plays in the digital economy. The lack of engagement with the policy community, in turn, translates to a lack of consideration for the unique needs and perspectives of the OSS ecosystem, its methodologies, and the socio-economic impact of OSS solutions. Congress participants argued that regulations such as the CRA assume proprietary software development as the default and have not properly understood or accounted for the distinct characteristics of OSS, including its development and licensing models. European OSS leaders in attendance predict that the documentation, certification, and liability provisions of the CRA could have a chilling effect on OSS development.[5] Meanwhile, a more inclusive regulatory process that accounts for the unique dynamics of OSS development and distribution could enhance cybersecurity and benefit the open source ecosystem.

Policy advocacy and education are critical to the continued success of the open source ecosystem

Congress participants' greatest fear is that policymakers don't understand how the open source ecosystem operates and are introducing regulations and policies that wittingly or unwittingly risk breaking the collaboration model that makes the community successful. Several foundation leaders noted that policymakers are not necessarily deep experts in everything they regulate, so they depend on the expertise of people inside the industry. In some cases, the absence of a coordinated open source response to major technology policy issues has created a void and ultimately left the playing field open to domination by larger, better-resourced entities.

Generally, OSS foundations are not resourced to run full-time government relations organizations. Nevertheless, OSS foundations have been active on major policy issues. Several foundation leaders recalled doing hours and hours of work on educating policymakers about open source components in the wake of the Log4Shell security incident but noted that those efforts merely scratched the surface. There were numerous calls for OSS foundations to invest more in educating the policy community about the benefits of open standards and open source.

Congress participants identified several critical issues around which policymakers require education. For example, what is an open standard? How do open source revenue models work? How does OSS impact competition and choice in the software market? And, how do policies around Internet security, product liability, and intellectual property (to name a few) impact open source production and distribution models?

The open source leaders assembled in Geneva were broadly supportive of establishing cordial and mutually beneficial relationships with policymakers and regulators. However, Congress participants also warned that the OSS community must be alert to the potential weaponization of standards. One participant noted that standards have long been used as an element of national economic strategy, where efforts to align standards around domains of technological superiority can confer a national competitive advantage. As such, there is a risk that some actors will co-opt standards processes as a means to further national interests and technology leadership goals instead of letting open standards development run its course. The reality that state actors may weaponize OSS to advance geopolitical agendas underscores the need for community members to join forces in defending the neutrality of OSS and highlighting its vital role as a collective knowledge base for all of humanity.

Effective policy work requires specialized skills and increased collaboration between OSS foundations

A recurring theme during the discussions in Geneva was the notion that policy advocacy differs significantly from OSS development work and requires specialized skill sets and increased community collaboration. Several Congress participants noted that there is often a disconnect between engineers who work on software and the policy people who work in regulatory institutions such as the European Commission. As such, the onus is on OSS foundations to acquire the skill sets and knowledge required to engage in policy deliberations, including a nuanced understanding of how regulatory institutions create policy. Other vital competencies include legal acumen and an intimate familiarity with the regulatory landscape, the ability to communicate complex technological concepts to non-technical audiences, and skills in advocacy, public speaking, and community engagement to help raise awareness and garner support for specific technology policies.

Congress participants agreed that influencing policy change that will benefit the open source ecosystem requires not only a long-term commitment to building capacity but also investments in building relationships with the policy community. Several participants argued that influencing policy can be a lengthy process, often requiring persistence and the ability to work toward long-term policy goals. Many of the OSS foundations present in Geneva also noted that they are currently under-resourced for policy work. Although some OSS foundations are hiring professional lobbyists, there were suggestions that foundations could draw additional support from their member companies, many of which have extensive and well-funded government relations operations. As one participant noted, "We are seeing higher levels of engagement in policy circles, but we need more resources and more sustained efforts to build the relationships."

In the end, OSS foundation leaders agreed that more community-wide collaboration on policy will be essential to the community's success in influencing policy agendas. The general sentiment was that OSS foundations have excelled when collaborating on software development but have been poor when it comes to collaboration on policy and governance. Many would like to see open source foundations come together to propose new policies around cybersecurity, AI, privacy, intellectual property, and other pertinent matters. Congress participants also agreed that more discussion is required to forge connections between various policy teams, build increased capacity for policy advocacy across the community, and establish a structure for cross-foundation collaboration on policy issues. As one participant put it, "We need to understand each other better, including our charters and member concerns and our efforts to influence policy, so that we can better coordinate our efforts as foundations."

The onus is on OSS foundations to acquire the skill sets and knowledge required to engage in policy deliberations.

Keeping Collaboration Global, Open, and Inclusive: Examining the Impact of Export Controls, Digital Sovereignty, and DEI

For decades, unfettered global collaboration on OSS development has swelled the ranks of talented developers contributing to open source projects. In 2022, more than 83 million developers from over 200 countries contributed to open source projects on GitHub. Significantly, some 74% of GitHub's global user base resides outside of the United States, with a significant increase in the share of developers based in Asia, Latin America, and Eastern Europe. Meanwhile, several breakthrough OSS innovations have come from places such as Japan (Ruby), Finland (Linux), and South Africa (Ubuntu).

While open source has seen unprecedented global success, the community leaders gathered in Geneva expressed concerns that global trade tensions, geopolitical conflict, and an increased focus on digital sovereignty pose genuine obstacles to open and inclusive collaboration. Rising techno-nationalism, for example, has prompted the United States, China, and other countries to tighten export controls over critical technologies, including semiconductors, unmanned aerial vehicles, global positioning systems, and various military electronics and software systems. Community leaders debated whether techno-nationalist policies could balkanize OSS development into regional silos and frustrate efforts to foster greater inclusion and deepen the community's talent pool.

In light of these risks, Congress participants weighed various options to help maintain the free flow of knowledge and technology across borders. Congress participants also discussed measures to enable open source project leaders to integrate diverse participants and successfully promulgate open source norms, ethics, and best practices.

Digital sovereignty poses opportunities and challenges for open source

Digital sovereignty was a key topic of debate in Geneva, including the degree to which initiatives to increase national control over digital technologies and data flows will either facilitate or impede the open source movement. Digital sovereignty refers to a country's ability to control its digital technologies, data, and information flow within its borders without undue influence from foreign governments or corporations. It encompasses the notion that a nation should have the authority to make decisions about its digital infrastructure, policies, and regulations in a manner that aligns with its own values, interests, and security concerns.

In recent years, various countries have introduced digital sovereignty measures, often motivated by concerns over data privacy, national security, economic growth, and the desire to reduce dependence on foreign technology providers. For example, Russia and China have introduced laws that mandate the localization of data within their borders and invested in building their own cloud infrastructure to store and manage data within their borders. Meanwhile, the European Union implemented the pathbreaking GDPR in 2018 to ensure greater data protection and privacy for their citizens. The GDPR was followed by the Digital Markets Act, the Digital Services Act, and the European Chips Act, which, together with the impending E.U. AI Act, constitute a sweeping set of digital sovereignty initiatives. The aim of these new laws is not only to uphold the rights of E.U. citizens in the digital space but also to increase the competitiveness of European companies in their efforts to compete against large U.S. tech firms.[6]

While digital sovereignty aims to provide countries with more control over their digital landscapes, it can also lead to challenges such as fragmentation of the Internet, barriers to cross-border data flows, conflicts with international norms, and increased regulatory compliance burdens for software developers and technology companies. Community leaders assembled in Geneva argued that digital sovereignty is often at odds with the goal of regulatory harmonization. Open source foundations understand that there will always be differences in how various nations and cultures address technology policy issues. However, the proliferation of new regulations increases the costs of compliance, with leaders noting that it is challenging for under-resourced OSS foundations to keep abreast of technology policy developments around the world. As one participant put it, “Open source runs the risk of being collateral damage in the rush to regulate the software industry as a whole.”

On the upside, several participants in the Open Source Congress suggested that digital sovereignty efforts could benefit the open source community. For example, in pursuit of digital sovereignty, some countries are embracing OSS to reduce dependence on proprietary technology. As a case in point, one Congress participant argued that the European Union will not achieve greater technology autonomy without leveraging open source and open standards, which would allow E.U.-based users to avoid vendor lock-in and gain more control over their technology stacks. In other words, Europeans do not necessarily have to own the source code to increase their digital autonomy when European leadership, in building and using open source solutions, provides an equally powerful remedy.

Techno-nationalist policies are causing some fracturing and siloing in open source communities

Digital sovereignty principally concerns the desire of national governments to increase their autonomy in managing digital infrastructure, policies, and regulations in a manner that aligns with nationally determined imperatives. However, Congress participants warn that, in some instances, the quest for digital sovereignty is becoming entangled in geopolitical rivalries and fomenting an atmosphere of growing mistrust, or what some analysts call techno-nationalism.

Alex Capri of the National University of Singapore defines techno-nationalism as “a mercantilist behavior that links a nation’s tech capabilities and enterprise with issues of national security, economic prosperity, and social stability.”[7] This new brand of techno-nationalism has seen countries worldwide move to restrict the transfer of critical innovations beyond national borders, believing that doing so will spur national economic growth and foster domestic competitive advantages. As a case in point, Capri cites “the steady progression of export controls on tangible, hard technology, followed by restrictions on data access and usage, and, most recently, new controls...that will impede the free movement and development of human capital.”

Techno-nationalism goes well beyond shoring up national autonomy to include more assertive measures to reign supreme in the technological sectors thought likely to dominate the 21st century, from robotics and AI to the industrial Internet and advanced telecommunications networks. The competition for national technological superiority among the world’s preeminent economies is so fierce that ecosystem leaders worry that geopolitical tensions and resulting policy interventions could slow technological progress and undermine the international collaboration on which the OSS community depends.[8]

For decades, technology has driven increased interconnectivity and global collaboration, of which OSS is a shining example. Congress participants noted that global collaboration has become fraught with political peril in today's environment, including once innocuous decisions about where to locate an open source conference. In some cases, companies headquartered in Western nations have been unwilling to participate in international open source projects in which companies from geopolitical rivals are also present because of the perceived legal uncertainties and the risk of a policy backlash at home. In other cases, international conflict or sanctions have resulted in contributors of various national origins being excluded from open source communities.[9]

Participants raised several critical questions about the impact of techno-nationalist policies and proclivities on the dynamics of participation and community management in the open source ecosystem. For example: How do we collaborate openly with companies on the "entity list" (a list of foreign persons and organizations maintained by the U.S. Department of Commerce to restrict the export of certain sensitive technologies and components to organizations involved in activities that threaten the national security or foreign policy interests of the United States)? How do we address security policies with contributors from various countries that may be suspected of being untrustworthy? As foundations, how should we intervene when contributors are being harassed because of their national origin in the wake of the Russian aggression against Ukraine?

Discussions in Geneva fell short of resolving some of the thorny issues raised by heightened geopolitical tensions. However, Congress participants agreed on several imperatives:

1. There was consensus that open source foundations must fight against fragmenting the community and its key platforms along geopolitical lines and advocate for maintaining the free flow of knowledge, technology, and collaboration across borders.
2. Open source leaders want to avoid situations where political considerations begin to dominate otherwise technical decisions about who participates in open source communities, on what terms, and to what ends.
3. Congress participants noted that a politically neutral posture and transparent protocols for managing community contributions are the keys to ensuring that open source projects operate without geopolitical tensions influencing how and when they engage with talented developers.
4. There was broad agreement that holding an annual Open Source Congress would facilitate international dialogues and the sharing of best practices among OSS foundations representing different regions of the world.
5. Open source leaders also agreed that when engaging with politicians and regulators, OSS foundations should promote the message that countries that close off collaboration at national borders will be less successful than those that embrace global cooperation and its benefits.

> *Global collaboration has become fraught with political peril in today's environment, including once innocuous decisions about where to locate an open source conference*

Diversity and inclusion are an essential part of the landscape and conversation about open collaboration

Once firmly rooted in the United States and Western Europe, today's open source community is increasingly global and cosmopolitan. China, for example, is a significant consumer of and contributor to open source technologies. Not only do nearly 90% of Chinese firms use open source technologies, but Chinese users are also the second most prolific group on GitHub after users from the United States.[10] However, China is not alone. Many emerging economies contain large communities of open source developers, including India, Russia, Korea, and Ukraine. For low – and middle-income countries, engagement with open source communities is giving rise to new entrepreneurial ventures and accelerating the pace of economic development.

While open source is flourishing globally, open source leaders assembled in Geneva warned that language, culture, and a legacy of Western-centric institutions pose obstacles to their ability to maximize the participation of talented developers. Although the open source community is increasingly international, several Congress participants argued that organizations headquartered in the United States have outsized influence in shaping most open source projects. The hegemony of North American participants, in turn, can overshadow open source projects that originated in other parts of the world.

Congress participants feared that a failure to address diversity and inclusion issues is curtailing the global OSS ecosystem's access to talent and ingenuity, thereby undermining its capacity to maximize innovation, access, and social impact. As one participant explained, "The people who don't feel welcomed will build technology in other ways. Unfortunately, that could mean that the best talent will build proprietary technology because they don't have the time and resources to contribute for free."

The challenges of integrating different languages and cultures into open source communities are not new problems, and there is considerable confidence in the ecosystem's capacity to foster global inclusion. However, Congress participants agreed that the community can do more to promote global inclusion. For example, some participants underlined the need to invest in rapid machine translation capabilities for project communications. While English may be the lingua franca of the software world, OSS leaders insist that localizing project communications drives broader participation from developers from outside of North America.

Congress participants also discussed the importance of promoting open source norms, taming the industry's macho "bro" culture, and fostering professionalism in community dialogues and decision-making. Several participants noted that codes of conduct are vital tools for establishing community norms, fostering diverse participation and creating inclusive environments. However, codes of conduct have often been controversial in open source communities, which have been known to be fiercely protective of their freedom and autonomy. Occasional backlashes from the contributor community have made the enforcement of community norms and standards of behavior a delicate balancing act. Several foundation staff reported having been subject to harassment over the enforcement of codes of conduct. There was broad agreement in Geneva that OSS foundations should come together to work on a coordinated approach to creating and enforcing codes of conduct that will promote diversity and inclusion in the community.

Does AI Change Everything? What Is Open? Liability, Ethics, Values.

Artificial intelligence can be defined as the ability of computers to perform tasks that had previously required human intelligence, such as perception, learning, reasoning, complex problem-solving, and decision-making. It is a broad field that encompasses a wide range of techniques and approaches, including machine learning, natural language processing, computer vision, robotics, and expert systems.

In recent years, AI has become increasingly integrated into our daily lives. AI-powered applications and services, such as Generative AI, voice assistants, recommendation systems, and personalized advertisements—even personalized billboards—have become commonplace. However, the transformation of our digital experience is just the beginning. From robotic surgery to autonomous vehicles, from revolutionary biotech research to reading CT scans, the applications for increasingly smart machines will span healthcare, legal and financial services, transportation, construction, agriculture, manufacturing, and much more.

Today, there are a plethora of AI initiatives being launched by companies such as Google, Facebook, Microsoft, IBM, Tencent, Alibaba, AWS, and most major corporations with access to massive datasets and computing power. The International Data Corporation predicts a 26% compound growth rate of AI expenditures for the foreseeable future. Maintained for a decade, this snowballing investment would result in more than a 10-fold increase. It is not just software companies. In mid-2023, about 40% of all JPMorgan open positions were AI-related, for data engineers and quantitative analysts, as well as ethics and governance roles.

For the OSS community, AI presents an array of opportunities and challenges. The community leaders assembled in Geneva discussed the need to align on a definition of open AI and the challenges AI-enabled code generators create for licensing, security, and intellectual property. Finally, Congress participants also reflected on the broader societal impacts of AI and the role of the open source community in addressing issues such as bias, privacy, and existential threats to humanity.

Openness in AI entails more than just access to the source code

Discussions about the nature and meaning of openness in AI were a focal point in the discussions about the responsible development of AI. Congress participants wrestled with a series of associated questions. What are our expectations for responsible AI? Does having access to the source code qualify as being open? What degree of transparency is reasonable for developers of AI models and tools?

With OSS, the definition of openness is well-established. According to the Open Source Definition, OSS is software with source code that anyone can inspect, enhance, and distribute.[11] Additionally, there are frameworks, licenses, and legal understandings that govern the rights of developers and the rights of users with respect to the use, modification, and distribution of OSS.

The same OSS protocols and definitions do not seamlessly transfer to AI systems. As Stefano Maffulli writes in a recent blog post, “When you find a bug [in OSS code], you know who to blame, you know where to report it, and you know how to fix it. But when it comes to AI, do you have the same understanding of what you need to do in order to fix a bug, error, or bias?”[12] The answer, according to Maffulli and many Congress participants in Geneva, was an unequivocal no.

The field of AI primarily focuses on creating systems that can process and analyze data, learn patterns, and make decisions based on programmed rules and statistical models, or simply derive associations and thoughts from the data itself. The underlying models have been described as black boxes because the decision-making processes of neural networks are based on statistical probabilities inferred from trillions of data points and, as such, are beyond the scope of human comprehension. Merely looking at the source code in AI does not necessarily explain or shed light on why AI systems generate the outputs they do. Even AI developers concede that they cannot readily explain the outputs of AI systems they are developing.[13]

Congress participants in Geneva argued that increasing explainability means improving the capacity to express why an AI system reached a particular decision, recommendation, or prediction. Explainability is important because it increases the trustworthiness, safety, and accountability of the systems that increasingly shape life-changing decisions such as diagnosing disease or deciding who gets access to credit. As Roman V. Yampolskiy, a professor of computer science at the University of Louisville, explains in a recent paper, "If all we have is a 'black box,' it is impossible to understand causes of failure and improve system safety." Yampolskiy goes on to argue that placing faith in AI's answers in the absence of an explanation is the equivalent of treating AI as an Oracle system. The danger, says Yampolskiy, is that "we would not be able to tell if [AI systems] begin providing wrong or manipulative answers."[14]

Developing the capability for AI explainability, said Congress participants, requires understanding the model architecture, including the weights applied to different variables in the models and the types of data used to train it. Unfortunately, the more sophisticated an AI system becomes, the harder it is to pinpoint exactly how it derived a particular insight. Indeed, some AI experts have claimed there are trade-offs between AI performance and interpretability.[15] In other words, making AI models explainable could render them less effective because doing so implies the need to reduce model complexity (e.g., using decision trees or linear regression rather than deep neural networks) and train the models on smaller, more curated datasets.

Another confounding factor in making AI more transparent is the scale at which AI systems operate. As Maffulli explains, "The volume of data consumed and generated by AI is measured in terabytes and petabytes, which means that special hardware is required to perform speedy computations on data sets of this size… Unfortunately, the hardware required to build and run these big AI models is proprietary, expensive, and requires special knowledge to set up."[16] In short, the massive computing power required to run the models makes it difficult for third-party organizations to interrogate the outputs. Therefore, the answer to surfacing AI's limitations and biases may lie, in part, in having companies such as Google, Meta, and others submit their models and systems to outside auditing and reliability testing.

AI-generated code will create challenges in open source licensing, security, and regulation

Another key thread of discussion in Geneva concerned the growing prominence of AI-powered code generators in the world of software development. Over the past several years, new tools such as GitHub's Copilot and OpenAI's Codex have awed developers with their power to generate not just simple lines of code but fully coded functions based on a natural language prompt. Coding tasks that might have taken hours or even days can now be completed in seconds. Over time, the increases in productivity could be transformational, with GitHub estimating that AI coding could boost global GDP by $1.5 trillion by 2030.[17]

Like other large language models, AI code generators have been trained on massive datasets, including the vast open source code libraries hosted on GitHub and other platforms. The upside is that open source repositories include a wealth of diverse code written by developers around the globe. These repositories encompass a vast array of programming languages, paradigms, and application domains, rendering them a rich and exhaustive wellspring of real-world code for training AI models. In essence, they mirror the experience and collective intelligence of the worldwide developer community.

The downside, as Congress participants pointed out, is that the growing use of AI code generators creates a series of challenges related to licensing, security, and regulatory compliance. These challenges stem from the lack of provenance associated with the code generated by AI models. For example, OpenAI's Codex does not include information about the licensing schemes that govern the original code that informed the code snippets it generates. As a result, it can be challenging to ascertain whether the generated code is proprietary, is open source, or falls under some other licensing scheme. This opacity creates a risk of inadvertent misuse of proprietary or licensed code, leading to potential infringement issues. Similar concerns have been raised about whether AI code generators are reproducing bugs and security flaws that were present in the codebases they were trained on.[18]

The use of AI-generated code also raises questions about whether the new software applications they generate should be governed by an open source license because the AI code generators have been trained on enormous volumes of open source code.[19] In other words, should AI-generated code be considered a "derivative work" of open source codebases?

Discussion in Geneva did not ultimately resolve these conundrums. However, participants agreed that OSS foundations should collaborate on new frameworks for working with AI-generated code because it is likely that AI will be an ever-present tool in software development going forward.

Systemic risks from AI require an urgent, open source response

The massive investments in AI development promise rapid advancements, enabling AI systems to tackle increasingly complex challenges and positively impact various aspects of human life. At the same time, Congress participants warned that the growing influence of AI has given rise to new risks and ethical considerations related to bias, transparency, privacy, job displacement, and existential threats to humanity.

Take bias and discrimination. Artificial intelligence systems can inherit or amplify biases present in the data they are trained on. If the training data contains biased or discriminatory patterns, the AI system can reinforce and even exacerbate these biases, leading to unfair outcomes in areas such as hiring, lending, or criminal justice. Artificial intelligence systems trained on historical loan data, for example, could perpetuate discriminatory lending practices, resulting in unequal access to credit or loans for marginalized groups. Predictive policing systems that use AI algorithms to identify crime hotspots and allocate police resources have been criticized for disproportionately targeting minority communities.

Artificial intelligence–engendered discrimination could prove hard to detect and even harder to counteract because the biases are essentially baked into the data on which its models are trained. As noted above, the current lack of transparency into how AI models function makes it impossible to understand how AI systems arrive at their conclusions or predictions. How can one identify and address any potential biases when the decision logic and mountains of underlying data are nearly impossible to unpack or reverse-engineer?

Bias and discrimination are, in most cases, unintended consequences of training AI on data that reflect society's prejudices and power structures. However, technology as powerful as AI is inevitably going to lead to decidedly intentional misuse of its capabilities for malicious purposes. In fact, the AI, Algorithmic, and Automation Incidents and Controversies Repository suggests such abuses are already commonplace. The organization's most recent report found that the number of newly reported AI incidents and controversies was 26 times greater in 2021 than in 2012. The authors conclude that "the rise in reported incidents is likely evidence of both the increasing degree to which AI is becoming intermeshed in the real world and a growing awareness of the ways in which AI can be ethically misused."[20] Notable incidents in 2022 included a deepfake video of Ukrainian President Volodymyr Zelenskyy calling for his troops to surrender the fight against Russia and the unprecedented rise in the use of "bots" to manipulate everything from elections to the news agenda and social media. Very plausible near-term risks also include the possibility that malicious actors could commandeer cyber-physical systems for destructive ends, such as holding critical infrastructure to ransom, crashing fleets of autonomous vehicles, or turning commercial drones into face-targeting missiles.[21]

Bias, deception, job displacement, and AI-enabled crime and terrorism top a lengthening list of risks. However, the ultimate existential question may be whether humanity can even control AI now that the genie is out of the bottle. Most AI experts predict that AI systems will eventually reach a level of superintelligence—exhibiting intelligence surpassing that of humans. The potential timeline for superintelligence is a subject of considerable speculation and debate. However, once this occurs, AI systems could potentially prioritize their own goals and act in ways that are detrimental to humanity.

Given what is at stake, OSS leaders in Geneva welcomed the various efforts underway to better understand the challenges and ensure responsible development and deployment of AI technologies. Most notably, on March 29th, 2023, more than 5,000 in the AI community signed an open letter calling for at least a six-month pause on further development of large language models such as GPT-4 until the risks can be properly studied and mitigated. Notable signatories include Elon Musk, who co-founded OpenAI; Emad Mostaque, who founded London-based Stability AI; and Steve Wozniak, the co-founder of Apple, as well as engineers from Amazon, DeepMind, Google, Meta, Microsoft, and others.[22] The open letter called for "new and capable regulatory authorities," a "robust auditing and certification ecosystem," and "well-resourced institutions for coping with the dramatic economic and political disruptions" that AI may cause. They add: "Powerful AI systems should be developed only once we are confident that their effects will be positive and their risks will be manageable."[23]

The open letter is symbolic of the AI community's level of concern. However, the proposed moratorium raises as many questions as it answers, including whether a moratorium is even enforceable. Indeed, in the race for this soon-to-be multi-trillion-dollar industry, it seems unlikely that any government or company would unilaterally force its AI tech leaders to pause development and risk ceding a significant advantage to their rivals.[24]

For the OSS leaders assembled in Geneva, the key to the responsible development and deployment of AI is not necessarily a moratorium but rather a commitment to greater openness and transparency. While many of the largest developers of AI systems have argued for keeping their AI models closed, several Congress participants argued that developing AI models in the open has advantages. These advantages include increasing the number of eyes on the code and creating the transparency required to ensure that AI systems are trustworthy.

In short, the consensus emerging from discussions in Geneva is that openness in AI provides a better pathway to addressing AI's weaknesses and challenges. Some suggested that tech companies are pushing systems into deployment very quickly and then claiming they will deal with bias and other problems as they are discovered. Open source leaders insisted that the AI community should commit to a higher standard of responsible development. Responsible development includes training AI systems on diverse datasets and baking ethics, safety, and algorithmic transparency into AI models from the outset, not as an afterthought. Additional measures could include guidelines for data collection, rigorous testing protocols, and auditing practices to mitigate bias and discrimination. As one participant put it, "The notion that AI developers can't explain the output of large language models is no longer acceptable. We need to push the technical boundaries to make the outputs transparent and explainable."

As the underlying technologies mature, AI will perform an ever-increasing array of tasks that today require human intelligence, such as learning, reasoning, problem-solving, perception, and decision-making. Groundbreaking applications in domains such as healthcare, transportation, public administration, finance, education, and entertainment will give rise to significant social and economic benefits but also considerable risks. As companies race to deploy and monetize a new generation of AI technologies, it would be prudent for all stakeholders involved in AI development to commit to ethical guidelines or principles for AI development that promote transparency, accountability, fairness, and the responsible use of AI technology, ensuring that AI systems align with human values and societal well-being. Above all, a commitment to open source approaches would ensure that AI is deployed in a manner that aligns with human values, safeguards human rights, and promotes the overall well-being of society.

Groundbreaking applications in domains such as healthcare, transportation, public administration, finance, education, and entertainment will give rise to significant social and economic benefits but also considerable risks. As companies race to deploy and monetize a new generation of AI technologies, it would be prudent for all stakeholders involved in AI development to commit to ethical guidelines or principles for AI development

The Imperative for Open Source Collaboration

Morning discussions among open source leaders in Geneva delved into several key challenges facing the open source ecosystem. One participant colorfully described these challenges as the four existential threats to open source collaboration: cybersecurity and the resilience of critical infrastructure; new and emerging regulatory initiatives that threaten the open source model; growing techno-nationalism and the need to foster diverse participation in open source projects; and the implications of AI for open source licensing, security, and intellectual property.

An overarching theme across each of these domains was the need for increased collaboration among OSS foundations and other key stakeholders in the global open source ecosystem. In the afternoon, the focus turned to how to bring key stakeholders together to address the urgent challenges facing the open source community.

Identifying shared priorities for the open source ecosystem

Before working through the potential mechanics of collaboration, Congress participants recapped the core issues around which greater cooperation is needed.

- **Securing open source infrastructure.** Congress participants would like OSS foundations to collaborate on maturing the ecosystem's approach to managing cybersecurity concerns. Key priorities include dedicating more resources to maintaining critical OSS infrastructure, building a deeper talent pool of cybersecurity professionals, and moving to a security by default model with enhanced capabilities for automated testing, patching, and auditing. As one participant put it, "If we don't figure this out, we will see a growing amount of regulatory scrutiny."

- **Increasing policy collaboration to safeguard the open source development model.** In the wake of increasing regulatory scrutiny, open source leaders called for OSS foundations to implement a proactive stance on policy engagement and to engage much earlier in the policy deliberation process. Congress participants urged OSS foundations to recruit experienced policy strategists and to forge greater alignment on key issues. "We need to confront threats through collaboration," said one participant. "A bigger army behind open source would help advance our values and imperatives."

- **Broadening policy engagement.** Open source leaders would also like to see OSS foundations be more inclusive of the large constituencies that have been largely left out of many policy collaborations. Participants noted that there are many policy collaborations occurring between organizations in the U.S. and Europe, while China, India, and Brazil, for example, have huge numbers of contributors but very little engagement in policymaking. "We must build bridges across countries and bring other voices into the conversation," said one participant.

- **Preventing regional fragmentation.** Congress participants were largely sympathetic to national efforts to increase digital sovereignty. Some see a substantive role for OSS in enabling countries to wrest greater control over their data and digital infrastructure. However, open source leaders are concerned that global trade tensions and geopolitical conflict pose genuine obstacles to open and inclusive collaboration and want OSS foundations to work together to avoid regional fragmentation and silos in open source projects.

- **Promoting inclusion by aligning codes of conduct for open source communities.** Congress participants suggested that aligning code of conduct language across the community could help to create shared expectations and norms for OSS projects. Others called for external enforcement support, such as convening a community of neutral peers to help adjudicate code of conduct issues. While there was also some support for a common code of conduct template for OSS foundations, several participants noted that any template must be flexible enough to accommodate regional and cultural differences.[25]

- **Managing the opportunities and challenges of AI.** Like many other fields of endeavor, AI is bringing sweeping changes to software development. Congress participants agreed that the OSS community needs a collective approach to AI because it changes everything about how developers generate open source code. Areas for collaboration include creating a data commons for training large language models and examining the impact of AI on licensing and intellectual property. Congress participants would also like to forge alignment on how the community defines open AI, which many agree presents a better pathway to managing the socio-economic risks and challenges associated with increasingly powerful AI systems.

While it is natural and ultimately vital to focus collective attention on threats to the open source model, Congress participants also identified a need to be more vocal about the public benefits that the open source community has produced—from the essential underpinnings of the Internet to the vast cloud of powerful software solutions for everything from running a business to addressing humanity's most urgent challenges. Congress participants urged OSS foundations to band together to preserve and enhance the technology commons that developers around the world have contributed countless hours to building. As one participant put it, "As a community, we are aiming at something much bigger than just cost-effective software, we are engendering control over software and computing. We need to be global in our orientation and our impact."

Creating a structure and process for effective collaboration

Having identified a set of shared priorities for the global open source community, Congress participants focused their attention on the mechanisms for enabling collaboration. In working through the options, open source leaders posited two potential models for collaboration.

- **A global secretariat for open source.** Several Congress participants made a case for a new global secretariat, or what some described as a United Nations for the open source community. Advocates for a new global entity noted that most industries have international associations that produce collective goods and lobby on behalf of their membership. The open source community, on the other hand, has a large and diverse collection of regional, sector-based, and project-based foundations that cater to the needs of their unique constituents. However, the ecosystem lacks an overarching structure or organization to advance the shared interests of the community. One participant suggested that today's ad hoc approach to inter-foundation collaboration is haphazard and makes the OSS community appear unprofessional and unorganized in its approach to regulation and policy.

  Congress participants debated whether it would be possible to thrust an existing organization into a global stewardship role on behalf of the community. As some pointed out, established OSS foundations have well-defined mandates and resources to deliver against the priorities identified by their member organizations. As such, they are not necessarily equipped or funded to play a larger global coordinating and advocacy role for the ecosystem as a whole. However, several participants noted that the Open Source Initiative, through its Open Policy Alliance, is already working with a coalition of partners to inform public policy decisions related to OSS, content, research, and education.[26] As one participant explained, “We need something that is truly global and representative. It would be nice to have a secretariat with resources, deep policy expertise, a neutral positioning, and a mandate to be of service to the entire ecosystem.”

Those speaking in favor of a new global secretariat raised concerns about the limited bandwidth at existing OSS foundations to address collective, ecosystem-wide challenges. While there was no shortage of good intentions expressed regarding the need to deepen collaboration across the ecosystem, some fear that inter-foundation cooperation could be sidelined by the day-to-day grind to deliver on existing mandates. In general, funding for collaborative efforts among OSS foundations is limited. As one participant argued, “If it’s not someone’s job, it won’t get done.”

- **A lightweight, peer-to-peer network for collaboration.** On the other side of the debate were those who argued that a network of OSS foundation executive directors—or, in some instances, a peer group of policy leads—would be sufficient to accomplish many of the critical needs of the ecosystem. Congress participants in favor of a lightweight approach to ecosystem collaboration were skeptical of the benefits of establishing a new global entity that would require a significant investment in people and infrastructure. They noted that there are already several meta-organizations in the ecosystem. Moreover, they placed faith in the capacity of existing OSS foundation leaders to come together at regular intervals, identify shared priorities, and distribute responsibility for managing collaborative efforts.

It was clear by the conclusion of the discussions in Geneva that further conversations would be required to define the best path for structuring ecosystem-wide collaboration. Regardless of the mechanism, there was broad support for continuing the conversations that started in Geneva. In the short term, Congress participants said that sustaining momentum was critical. Several suggested that a series of inter-foundation working groups equipped with simple tools for collaboration could make progress on issues such as cybersecurity, regulation, and open AI.

There was also strong support for holding an annual Open Source Congress, with participants broadly agreeing that they see tremendous value in regularly convening leaders of OSS foundations and other stakeholders. As one participant put it, “Today, we are fragmented as organizations, but we can be much more powerful when we are united.”

Going forward, there was a consensus that greater inclusion in open source governance is paramount. Participants from outside of Europe and North America observed that many of today’s open source gatherings are Western-centric. They would like to see inclusive processes that include real-time localization. There was also broad support for rotating an annual Open Source Congress through traditionally under-represented regions of the world.

Congress participants would also like the community of established OSS foundations to offer more support to emerging foundations. For example, in Asia, Africa, and Latin America, there are expansive developer communities and many ad hoc user groups but very few formal foundations. To facilitate greater inclusion in governance and policy engagement, more regionally focused foundations may be required to represent these constituencies. Several participants suggested that an onboarding process for new foundations could help transfer knowledge from mature foundations to emerging OSS organizations. A peer network and an index of foundations would also help new foundation leaders feel more connected to the ecosystem.

Conclusion

In the end, Congress participants agreed that the time and resources devoted to coming together in Geneva were well invested. Open source leaders from around the world had a chance to meet in an intimate setting, many getting to know each other for the first time. Subject matter experts hashed out critical issues on panels. Shared priorities were identified and discussed. Options for deepening ecosystem-wide cooperation were proposed and debated. Above all, participants cemented their resolve to continue the conversations and deepen the collaborations going forward.

The ultimate proof of the pudding, of course, is in the eating. Now it is up to the ecosystem's leaders to rally behind the imperative to collaborate and to continue the vital work of the open source community. Rising techno-nationalism, new regulations, and novel cybersecurity threats will pose challenges. A more united and collaborative open source community will be more successful in resolving them. The OSS foundation leaders assembled in Geneva are committed to leading the charge, and more will surely join them. As one participant aptly declared, "The collaboration we are doing here is to support the hundreds of thousands of developers who are producing billions of dollars of software and changing the world in the process."

Acknowledgements

The author would like to acknowledge the contributions of the 53 open source community leaders who gathered in Geneva and whose insights and commentary inspired this report. I am grateful to Chris Xie at Futurewei, whose leadership and contributions made the Open Source Congress possible, and to the Linux Foundation team for hosting an inspiring event and publishing this report. A warm thank you to Jerry Michalski for your teamwork in laying the intellectual groundwork for the Congress and for animating the community conversations in Geneva. I would also like to offer special thanks to those who took the time to review early drafts and provided valuable advice and insights, including Omkhar Arasaratnam, Stella Biderman, Mirko Boehm, Jory Burson, Thierry Carrez, Stefano Maffulli, Mike Milinkovich, Deb Nicholson, and Rebecca Rumbul.

About the author

Anthony is the founder and president of the DEEP Centre and an internationally recognized authority on the digital revolution, innovation, and creativity in business and society. He is co-author (with Don Tapscott) of the groundbreaking bestseller Wikinomics and its follow-up Macrowikinomics: New Solutions for a Connected Planet.

Among other appointments, Anthony serves as a research director with the **Blockchain Research Institute**, an expert advisor to the **Markle Foundation**'s Initiative for America's Economic Future, and a senior fellow with the **Lisbon Council** in Brussels. Anthony was recently a committee member of the National Research Council's Committee on **Science for the EPA's Future**, a visiting fellow with the **Munk School of Global Affairs** at the University of Toronto, and chief advisor to Brazil's Free Education Project. His work on technology and innovation has been featured in publications such as the Harvard Business Review, the Huffington Post, and The Globe and Mail.

References

1 https://academic.oup.com/book/44727/chapter/378967711

2 https://linuxfoundation.eu/newsroom/the-rising-threat-of-software-supply-chain-attacks-managing-dependencies-of-open-source-projects

3 https://www.cisa.gov/resources-tools/resources/cisa-open-source-software-security-roadmap

4 https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on#:~:text=Introduction,and%20non%2Dtech%20companies%20alike.

5 https://newsroom.eclipse.org/news/announcements/open-letter-european-commission-cyber-resilience-act

6 https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

7 https://thediplomat.com/2020/09/us-china-techno-nationalism-and-the-decoupling-of-innovation/

8 https://www.channelnewsasia.com/business/risc-v-group-says-restrictions-open-technology-would-slow-innovation-3833631

9 https://www.computer.org/publications/tech-news/community-voices/on-the-weaponization-of-open-source

10 https://merics.org/en/short-analysis/china-bets-open-source-technologies-boost-domestic-innovation

11 https://opensource.com/resources/what-open-source

12 https://opensource.com/article/22/10/defining-open-source-ai

13 https://www.vice.com/en/article/y3pezm/scientists-increasingly-cant-explain-how-ai-works

14 https://philarchive.org/archive/YAMUAI

15 https://www.linkedin.com/pulse/interpretability-vs-performance-trade-off-balancing-model-shirsat

16 https://opensource.com/article/22/10/defining-open-source-ai

17 https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/

18 https://www.wired.com/story/fast-forward-power-danger-ai-generated-code/

19 https://www.lexology.com/library/detail.aspx?g=4d3d8be3-abeb-430b-a7ab-bae434d3e014

20 https://aiindex.stanford.edu/report/

21 https://www.cam.ac.uk/Malicious-AI-Report

22 https://www.theguardian.com/technology/2023/mar/29/elon-musk-joins-call-for-pause-in-creation-of-giant-ai-digital-minds

23 https://www.bloomberg.com/opinion/articles/2023-04-05/an-ai-pause-would-be-a-disaster-for-innovation

24 https://www.brookings.edu/blog/techtank/2023/04/11/the-problems-with-a-moratorium-on-training-large-ai-systems/

25 Potential models for a shared code of conduct template include:
OpenSSF: https://openssf.org/community/code-of-conduct/
CC: https://opensource.creativecommons.org/community/code-of-conduct/
Meta: https://opensource.fb.com/code-of-conduct/
Amazon: https://aws.github.io/code-of-conduct

26 https://opensource.org/programs/open-policy-alliance/

THE LINUX FOUNDATION | Research

Founded in 2021, **Linux Foundation Research** explores the growing scale of open source collaboration, providing insight into emerging technology trends, best practices, and the global impact of open source projects. Through leveraging project databases and networks, and a commitment to best practices in quantitative and qualitative methodologies, Linux Foundation Research is creating the go-to library for open source insights for the benefit of organizations the world over.

To reference this work, please cite as follows: Anthony Williams, “Standing Together on Shared Challenges: Report on the 2023 Open Source Congress,” foreword by Yue Chen and Chris Xie, The Linux Foundation, December 2023.