Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109 USA
415.436.9333
eff.org

Comments of the Electronic Frontier Foundation on the CMA's Inquiry on Mobile Browsers and Cloud Gaming

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows. EFF represents tens of thousands of dues-paying members, including consumers, hobbyists, artists, computer programmers, entrepreneurs, students, teachers, and researchers.

We submit these comments in response to the Competition and Markets Authority's (CMA) inquiry on the markets for the supply of mobile browsers and cloud gaming in the United Kingdom. This comment will primarily address the supply of mobile browsers in the U.K. The CMA's study has concluded that Apple and Google's duopoly on mobile ecosystems means they have a stranglehold over key gateways. The CMA identified that there are many potential interventions which could help unlock competition and protect millions of businesses and people reliant on their services. The CMA is taking action now to tackle the many problems it has identified, and the new pro-competition digital regime expects to have additional powers to oversee these key digital markets.

Mobile devices with internet connectivity play a fundamental role in the lives of people in the U.K.—providing fast and convenient access to a wide range of products, content and services. Mobile browsers are a crucial gateway for people to access the web from mobile devices and are one of the most used apps on users' phones. Browser engines are the critical technology that enables browsers to load and display web pages. They are fundamental to the performance and capability of a browser. Apple and Google have substantial market power in both mobile browsers and browser engines. In 2021, 97% of all mobile web browsing in the UK was performed on top of either Apple's or Google's browser engine. Apple and Google have key advantages over other browser vendors, such as Chrome or Safari being pre-installed on mobile devices, which firmly entrenches each company's competitive advantage.

Due to Apple and Google's tight grip over mobile browsers and browser engines, competition is stifled, and consumers are likely to miss out on new innovations. The CMA should encourage a further examination of Apple and Google's stewardship over mobile operating systems and exercise its discretion in providing appropriate remedies.

1) Do you consider that our analysis is correct with respect to the suspected features of concern in the supply of mobile browsers and cloud gaming in the UK?

The CMA's analysis with respect to the suspected features of concern regarding mobile browsers and cloud gaming in the U.K. is correct and substantiated. The CMA's study identified that Apple and Google have a stranglehold over key gateways. The three browser engines with material market share, Apple's WebKit, Google's Blink, and Mozilla's Gecko, compete for users, browsers, and online content providers.[1] Apple's Safari and Google's Chrome are the most-used browsers on mobile devices, with a combined market share of around 89% on mobile devices in the U.K.[2] Mobile browsers serve as a critical vehicle for developers to build innovative web pages and web apps in order to attract users and help businesses grow.[3]

Apple does not allow competing browser engines on its devices and has lagged behind the competition in implementing a wide range of key features. For example, Apple restricts the use of certain web features on its devices, such as push notifications and full screen functionality, potentially hampering the development and take-up of web apps.[4] Google has fewer explicit restrictions, but it still exerts significant control over its mobile app store, and its many products and services are built to drive and reinforce the use of other Google services.

Apple has a history of invoking security as a procompetitive rationale for its policies, when many of the company's practices are, in fact, anticompetitive. Apple's security rationale for its App Store policies does not overcome the harm those policies cause to innovation, including innovations that would enhance consumers' security and privacy.[5] Apple sets 'the rules of the game' when it comes to its mobile operating system and the App Store. The company places restrictions on both the functionality and the expressive contents of apps, and refuses or delists apps that transgress these restrictions.[6] The company's policies also thwart developers' attempts to meet user needs relating to privacy, security, and access to information.[7] Finally, Apple's paternalistic approach to security and privacy led to the company banning apps and features that would serve a

[1] CMA Mobile Ecosystems Market Study Final Report, Section 5.21, p. 147-148
[2] CMA Mobile Ecosystems Market Study Final Report, Section 5.24, p. 148
[3] CMA Mobile Ecosystems Market Study Final Report, Section 5.34, p. 151
[4] CMA Mobile Ecosystems Market Study Final Report, Section 5.61, p. 158
[5] EFF Amicus Brief for Epic Games v. Apple, p. 12
[6] EFF Amicus Brief for Epic Games v. Apple, p. 13
[7] EFF Amicus Brief for Epic Games v. Apple, p. 17

wider range of those needs, like VPN apps for international travelers and apps that tell the user if their device has been jailbroken.[8]

Apple and Google's app stores are the two main gateways for app developers and users to unlock the value of mobile devices. Both Apple and Google unilaterally determine the terms of access to their app stores and set high commission rates.[9] Both companies have exploited their power to unfairly favor certain businesses over others.[10] Interventions are needed to transform these markets, enable innovation, and improve privacy and security. This inquiry will promote a pro-competitive regulatory regime, and allow the CMA to take targeted action to improve the digital markets.

EFF has long held that "code is speech" – a principle established in one of our oldest and most significant court battles[11]. Accordingly, EFF believes that governments should tread lightly when mandating software and hardware characteristics, and that any state order that forces a manufacturer or software author to implement or refrain from implementing a particular technology or tool represents an incursion on free expression rights.

Historically, EFF counseled that the correct remedy for badly run or anticompetitive app stores is to allow third parties to offer competing apps and app stores. However, the dominant mobile platform vendors have woven together a thicket of legal doctrines—including anticircumvention elements of copyright law, software patent, trade secret, badly drafted cybersecurity laws, onerous contract terms, and exotic tortious interference theories at common law—that create unbearable legal risks for anyone who would offer device owners alternative app stores.

The U.K. (as well as the US, EU, and other jurisdictions) are ripe for comprehensive legal reform, in order to return to the owners of devices the right to decide how they are configured and used, and which software will run on them. However, such an effort is extremely fraught, and is the domain of legislators, not competition regulators.

Accordingly, EFF believes that regulators have a role to play in restoring device owners' rights with targeted interventions in the practices of gatekeeping technology vendors and services. We believe that these interventions should be cautious and minimally invasive, representing the least proscriptive measures that will safeguard users' rights. For example,

---

[8] https://www.eff.org/deeplinks/2022/02/eff-appeals-apples-monopoly-doesnt-make-users-safer
[9] CMA Mobile Ecosystems Market Study Final Report, Section 7.66, p. 272
[10] https://www.eff.org/deeplinks/2020/06/apples-response-hey-showcases-whats-most-broken-about-apple-app-store
[11] https://www.eff.org/cases/bernstein-v-us-dept-justice

it would be better to order support for alternative app stores than to mandate that existing app stores must carry specific apps.

EFF believes that mandating support for alternative browsers and browser engines meets these criteria; indeed, because such a measure could promote robust Web App support, it could fill the same need as a mandate for alternative app stores with a more parsimonious and less invasive measure.

---

2) Do you consider that our analysis is correct with respect to the reference test being met in relation to the supply of mobile browsers and cloud gaming in the UK?

In its guidance on making MIRs, the CMA sets out four criteria which help to guide them in determining whether the regulator can exercise its discretion: (1) the scale of the suspected problem; (2) the reasonable chance that appropriate remedies would be available; (3) whether it would be more appropriate to address the concerns through alternative means; (4) whether it would more appropriate to address the competition problems through the CMA's alternative powers, or through the power of sectoral regulators.[12] (Final Report, 9.5, 340) Through their market study, the CMA has identified several competition concerns regarding Apple and Google's mobile browsers, browser engines, and cloud gaming policies. The CMA's analysis with respect to the reference test regarding the supply of mobile browsers in the U.K. is correct and substantiated by the analysis provided in the Mobile Ecosystems Market Study Final Report.

Apple and Google hold a *de facto* duopoly over operating systems, app stores, and browsers for mobile devices.[13] Apple's Safari and Google's Chrome are the most-used browsers on mobile devices, with the combined share of these two browsers on mobile devices amounting to 90%.[14] Apple requires all browsers on iOS to use Apple's own Webkit as their browser engine.[15] Through this restriction, Apple maintains sole control over the feature set not only for its own browser, but for all browsers on iOS, which restricts competition and also limits the capability of all web applications on iOS devices.[16]

---

[12] CMA Mobile Ecosystems Market Study Final Report, Section 9.5, p. 340
[13] CMA Mobile Ecosystems Market Study Final Report, Section 3.14, p. 33
[14] CMA Mobile Ecosystems Market Study Final Report, Section 5.24, p. 148
[15] CMA Mobile Ecosystems Market Study Final Report, Section 5.45, p. 153
[16] CMA Mobile Ecosystems Market Study Final Report, Section 5.57, p. 157

The types of interventions identified by the CMA could remedy this. The CMA could open up core markets in the mobile ecosystem by requiring Apple and Google to provide access for third parties in the mobile ecosystem, or restrict self-preferencing where anticompetitive effects are present.[17] Given the tight control both Apple and Google maintain through interconnections between each company's mobile products and services, the CMA could also consider separation remedies that require Apple and Google to operate certain lines of business independently.[18] The CMA could also consider the case for a requirement for Apple to allow alternative browser engines on iOS, or mandate minimum standards for browser functionality.[19]

EFF finds that the reference test has been met for CMA as a regulator to exercise its discretion when addressing the issues concerning mobile browsers. EFF takes no position in these comments on the CMA's proposal with respect to cloud gaming.

---

3) Do you agree with our proposal to exercise the CMA's discretion to make a reference in relation to the supply of mobile browsers and cloud gaming in the UK?

EFF supports the CMA's proposal to exercise its discretion to make a reference in relation to the supply of mobile browsers in the U.K. EFF takes no position in these comments on the CMA's proposal with respect to cloud gaming.

4) Do you consider that the proposed scope of the reference, as set out in the draft terms of the reference published alongside this document, would be sufficient to enable any adverse effect on competition (or any resulting or likely detrimental effects on customers) caused by the features referred to above to be effectively and comprehensively remedied?

We are confining our response to those aspects of this consultation that relate to browsers and browser engines and we are not commenting on the mobile gaming/cloud gaming elements.

EFF is confident that the draft terms of reference are adequate to capture both the colloquial and technical meaning of "browser" and "browser engine," and that in hewing to these references, the Authority will be able to make rules that address the competitive issues with both Web Apps and browser competition.

---

[17] CMA Mobile Ecosystems Market Study Final Report, Section 8.81, 8.11, p. 281-282
[18] CMA Mobile Ecosystems Market Study Final Report, Section 8.13, p. 282
[19] CMA Mobile Ecosystems Market Study Final Report, Section 8.116, 8.127, p. 308, 312

5) Do you have any views on our current thinking on the types of remedies that a MIR could consider (see above and Chapter 8 of the market study final report)? Are there other measures we should consider?

Once again, we are confining our response to those aspects of this consultation that relate to browsers and browser engines and we are not commenting on the mobile gaming/cloud gaming elements.

Owners of Devices Should Have the Final Say

EFF believes that owners of mobile devices should have the right to choose alternative browsers and alternative browser engines. We acknowledge that users may not always exercise this right wisely, and that evaluating an alternative browser or browser engine for suitability, security and robust privacy protections is beyond the capabilities of many users.

At the same time, EFF strongly believes that device manufacturers should not have the final say as to which software (including browsers, browser engines, and indeed, operating systems and the low level code needed to launch them, including bootloaders) can be used by device owners.

Manufacturers often make decisions in their users' interests, but sometimes they make decisions that are detrimental to their users' interests, particularly when the interests of their users conflict with their business priorities.

For example, Apple has a long and honourable tradition of standing by its users' privacy interests, as when the firm refused the FBI's demand to weaken the security of its operating system to enable forensic analysis[20].

But Apple also gave in to the Chinese authorities' demand to remove working VPN apps from its App Store[21], and exposed its Chinese users' iCloud data to state interception[22].

The Equilibrium of User Protection

Manufacturers' inconsistent conduct toward their users is best understood as an equilibrium that balances the firm's interests against the users'. Manufacturers may value their users' privacy, security and integrity, but they also seek profits for their shareholders.

[20] https://www.eff.org/apple-fbi
[21] https://www.eff.org/apple-china-vpn
[22] https://www.eff.org/china-apple-icould

When a juncture arises that forces manufacturers to balance their users' interests against their shareholders', manufacturers weigh the reputational and commercial costs of acting counter to their users' interests against the costs of acting counter to their shareholders' interest.

For example, when the FBI demanded that Apple assist them in defeating the security on an iPhone as part of a criminal investigation, Apple calculated that the costs of litigating its users' interests against the FBI were bearable relative in light of the harms to its users and the commercial losses it would suffer worldwide if the public came to believe that the FBI (and possibly other agencies) could break into Apple's phones.

Apple also doubtless factored in other costs, such as the risk that giving in to the FBI would set a precedent that other states around the world would invoke in their own demands to Apple, as well as the morale of its staff, many of whom chose to work for Apple in part to improve users' lives (there were almost certainly other elements of this calculus that outsiders will never be privy to).

When Chinese authorities demanded that Apple weaken its security, the firm factored in other costs and benefits, and arrived at a different conclusion. Again, it's impossible to know all the factors that Apple weighed up, but we do know that Chinese users represent a large market for Apple, and, perhaps more importantly, Chinese manufacturing is critical to Apple's operations. If noncompliance had cost Apple its ability to do business in China and source parts and finished goods from Chinese manufacturers, the company would have borne a high cost.

Apple is not unique in taking decisions that run counter to its customers' interests when its own interests are sufficiently implicated. But because of the closed nature of Apple's mobile iOS platform, Apple customers in China had few self-help measures available to them when Apple chose its shareholders' returns over its customers' safety. By design, Apple devices do not allow "sideloading" of apps, nor do they support third-party app stores. And, as the Authority's own report notes in great detail, Apple's mobile devices do not support powerful alternative browser engines that could circumvent network surveillance.

All of this is to explain that vendors *can* defend their users' security, but sometimes they choose not to, and sometimes vendors of complementary products will do it better. Therefore, to make a system that protects users, it is not enough to allow them to choose an OEM whose judgment they trust—we must also allow them to revoke that trust later and switch to aftermarket vendors, apps, OSes, software, add-ons, mods, and plug-ins that override the OEM's choices.

Property Rights and Mobile Devices

Ensuring that device owners have the final say over their devices is consistent with longstanding legal principles of private property as embodied in *Blackstone on Property*

(1753): "that sole and despotic dominion which one man claims and exercises . . . in total exclusion of the right of any other individual in the universe."

This technological self-determination is also a useful hedge against vendors' own errors in judgment or calculated trade-offs that sacrifice a customer's interests to protect the firm, for example, by allowing users to source working privacy tools if Apple revokes access to them in its official channels.

But enabling technological self-determination is also a means of shifting firms' own equilibrium when they seek to balance their own interests against their customers'. Walled gardens are a kind of moral hazard, because firms who know their users will incur high switching costs if they change vendors are emboldened to mistreat those users, calculating that users will endure a larger ration of maltreatment if the alternative is sufficiently burdensome.

As the comedian Lily Tomlin quipped in "The Phone Company," her classic 1976 *Saturday Night Live* sketch, "So, the next time you complain about your phone service, why don't you try using two Dixie cups with a string? We don't care. We don't have to. We're the Phone Company."

Creating space for alternative browsers and browser engines is a way to discipline the mobile duopoly, to change the microeconomics of their corporate boardrooms. When an executive says, "Well, it's a tough choice, but I think we should remove the working VPNs from our App Store;" another can counter, "Here's my estimate of how many of our users in China - and worldwide - will be spurred to switch to a rival browser if we do that."

The minatory effect of potential browser defections might be enough to stay Apple's hand and put its customers' interests ahead of its own—but if it's not, *those customers will be able to avail themselves of a rival browser*.

Protection Without Monopoly

If manufacturers can't be trusted with a veto over their customers' choices, and if users can sometimes be tricked into using poor-quality tools, then who should protect the public from deceptive practices and sharp dealing?

In "Privacy Without Monopoly," EFF Staff Technologist Bennett Cyphers and EFF Special Advisor Cory Doctorow articulate a theory of data protection that resolves this conundrum. Rather than abandoning the public to the inconstant and imperfect goodwill of tech companies, or the exigencies of a wide-open market, "Privacy Without

Monopoly" argues that freestanding, publicly accountable digital human rights legislation, backstopped by robust enforcement, is the answer[23].

In this formulation, any browser—indeed, any app or online service—would be measured against UK privacy and consumer protection law, with the ICO, FCA and other regulators empowered to take action against firms who offer defective products, engage in deceptive practices, or violate their users' privacy. This standard would apply to third parties who supplied browser engines and alternative browsers for the dominant mobile platforms—and it would apply to the manufacturers of the dominant platforms as well.

Security Matters

In any discussion of mandated interoperability, including the limited interoperability of alternative browser engines and browsers, incumbents can be relied upon to raise the spectre of security defects that the complexity of regulatory compliance will give rise to.

This is a very valid concern. Complexity is the enemy of security, and the seams where two systems join are often weaker than either of them on their own.

But secure interoperability *is* possible, and it requires much the same methodologies as securing single-vendor systems.

Apple and Google are already at pains to create firewalls within their mobile OSes to prevent applications from interfering with one-another. It's true that fully capable browsers need to have deeper integrations with the operating system than other sorts of apps, especially if they are to access hardware features such as Near Field Communication and Bluetooth chips.

Yet these are surmountable challenges. They have been met in other software contexts, including Android's browser support. As noted security expert and EFF Board Member Bruce Schneier wrote to the US Senate Judiciary Committee, in regards to proposed laws requiring competition in app distribution on mobile devices[24]:

> *Apple tries to imply that users who want to stay within its trusted ecosystem will be forced to take on new risks, or that non-technical users will be blindsided by new malware. This is simply not true. Side-loading could be implemented in a way that ensures users are aware of the risks they take on before installing a piece of unverified software. Users who do not want to side-load apps can easily choose not to, just as users today can choose not to jailbreak their phones. (Jailbroken phones are ones that have been modified in a way that contravenes Apple's rules to allow the installation of software the Apple prohibits.)*

[23] https://www.eff.org/interop-privacy
[24] https://www.eff.org/schneier-apple

Indeed, one of the significant benefits of allowing third-party browsers and browser engines is the possibility of users choosing *more* secure, *more* privacy-respecting alternatives to the duopoly's default browsers; for example, replacing Chrome with a browser that supports comprehensive and robust tracker-blocking; or replacing Safari with a browser that gets more timely security updates and can be patched without patching one's entire operating system, potentially breaking compatibility with other apps the user depends upon.

Administering a Browser Interoperability Order

In administering any interoperability remedy—especially a remedy involving low-level changes to the operating system, such as will be necessitated in order to integrate full-featured browser engines capable of supporting Web Apps—a regulator such as the CMA must be able to distinguish between pretextual security issues raised by recalcitrant gatekeepers, and bona fide security risks associated with ill-advised or reckless courses of conduct proposed by new market entrants hoping to field their browsers and browser-engines.

To do this, CMA must have a staff of in-house experts with extensive experience in security, browsers and mobile platforms, to sort through and adjudicate conflicting claims about security risks posed by new browsers and browser engines.

But such an adjudication is not a simple matter. It is fact-intensive and time-consuming, and apt to produce long delays. Simply raising pretextual security complaints and drawing out the fact-finding that followed may serve to discourage investors and technologists from attempting to produce the browsers and engines the Authority hopes to coax into existence through this intervention. Even if investors and technologists have the capital and patience to wait while the slow gears of justice grind away, their users may abandon their products and even the very idea of trying a third-party browser or engine as their favorite tools appear and disappear.

To compensate for this risk, EFF advises augmenting any mandate for gatekeeper mobile platform operators to accommodate third-party browsers and engines with a rule that permits third parties to add browsers and engines *without* availing themselves of the facilities gatekeepers choose to make available.

Rather, the Authority should empower third parties to engage in "adversarial interoperability[25]," which we also call "competitive compatibility" or "comcom." This is a suite of "guerilla" tactics for augmenting existing technologies, including reverse-engineering, scraping, automation via bots, and a suite of related techniques that the gatekeepers themselves have used throughout their own rise to power[26].

[25] https://eff.org/adversarial-interop
[26] https://www.eff.org/iwork-comcom

In practice, this would mean that the Authority would create an affirmative defense against legal claims by gatekeepers, which interoperators could invoke provided they could prove that the offending actions were in narrow furtherance of the goal of enabling device owners to choose alternative browsers and browser engines, and that the actions did not violate privacy laws or fair trading standards. This defense would immunise interoperators from claims under a variety of legal theories, including patent, copyright, trademark, anticircumvention, cybersecurity, and business tort theories.

When it comes to administering an interoperability mandate, comcom is a powerful aid. In general, the gatekeeper firms, like all listed companies, prefer to have an orderly and predictable market environment, not least because shareholders are prone to flash selloffs when presented with unexpected bad news[27]. Share volatility hits top executives—whose compensation is largely share-based—very hard, and also erodes the wage discount that large firms enjoy due to their ability to lure in high-demand workers with the promise of generous share grants.

Adhering to an interoperability mandate may erode a firm's monopoly profits, but it does so in a *predictable* and *managed* fashion. By contrast, engaging in hand-to-hand combat with new market entrants' comcom engineers presents *unquantifiable* risks of the sort that large firms are at pains to avoid, but which are relatively minor additional stressors in the endemically uncertain conditions of a new market entrant.

Adding comcom to a mandate takes away gatekeeper firms' stick—the threat of pretextual legal complaints—and demands that they perfect their carrots: high quality, highly reliable technological frameworks for integrating third party browsers and browser engines.

In an ideal world, the knowledge that inadequate or unreliable compliance with an interoperability mandate will result in new market entrants switching to comcom (openly circulating jailbreaking tools, say) will incentivise large firms to produce a congenial environment for those entrants.

But firms are not always rational, and it's possible that gatekeepers will decide that the risks of interoperators switching to comcom are worth the benefit of retaining monopoly control over their platforms. If that is the case, then interoperators will have comcom to fall back on, and will *still* be able to create the competitive outcomes the Authority is hoping to achieve.

---

[27] https://eff.org/fb-selloff

6) Do you have any views on areas where we should undertake further analysis or gather further evidence as part of an MIR in relation to the supply of mobile browsers and cloud gaming?

Once again, we are confining our intervention to those aspects of this consultation that relate to browsers and browser engines and we are not commenting on the mobile gaming/cloud gaming elements.

EFF wishes to reiterate that Apple and Google's concerns about the security of mobile platforms are well-founded. Governments around the world, including the U.K. government, have a long and dishonourable history of seeking to deliberately weaken the security of communications platforms in order to aid the efforts of law enforcement and security agencies. It has been less than a year since the U.K. government paid an ad agency £500,000 in public money to devise a smear campaign against end-to-end encryption, technology which creates a singular benefit to the privacy and security of all internet users[28].

Sabotaging the encryption of mobile platforms has grave consequences, far beyond the U.K.'s borders. Defects in mobile operating systems have been weaponized by unscrupulous cyber-mercenaries who sell mobile intrusion products to despots and autocrats around the world[29]. These, in turn, are used to in connection with ghastly human rights abuses, including the assassination of government critics[30].

These high stakes are a reminder that regulators should operate cautiously when mandating the functionality of mobile devices, and ensure that interoperability mandates strengthen rather than weaken the security of those devices.

But the existence of these cyberweapons and the long-festering defects they exploited also tell us that the gatekeeper firms should not have the last word when it comes to securing the devices they sell us. While gatekeepers' objections to interoperability mandates stress the risk of users unwisely choosing a vendor who makes their device *less* secure, there is little discussion of users who might choose a vendor who will make their device *more* secure.

The unfortunate decision of the European Commission to begin the work of the Digital Markets Act by mandating interoperability for end-to-end encrypted messaging tools[31] is a good example of how these pro-competitive efforts can go wrong.

By failing to forcefully require interoperators to retain specific security measures in their interoperability measures, the EU has opened up the real possibility that an interoperator

[28] https://eff.org/hmg-v-e2ee
[29] https://citizenlab.ca/tag/nso-group/
[30] https://citizenlab.ca/2018/10/the-nso-connection-to-jamal-khashoggi/
[31] https://eff.org/dma-v-e2ee

will field a product that puts their own users, and the users of a gatekeeper platform, at risk. Beyond the potential human consequences, there is also the potential for reputational harms to the notion of interoperability as a competition tool.

We suggest that plain, unequivocal security guarantees be written into any interoperability intervention on the Authority's part.

An MIR is an excellent vehicle for soliciting and sorting through competing proposals for such a guarantee. Security experts should be encouraged to submit concrete proposals for insulating mobile operating systems from third party browsers and engines, for ensuring the privacy of data "at rest" on users' devices, and for ensuring the integrity and privacy of communications via end-to-end encryption.

Respectfully submitted,

Cory Doctorow
Mitch Stoltz
Electronic Frontier Foundation[32]

[32] EFF thanks Legal Intern Shashank Sirivolu for his contribution to the drafting of these comments.