PROTECT THE STACK

Infrastructure Providers Should Not Be Content Police

स्टैक को सुरक्षित रखें: इन्फ्रास्ट्रक्चर प्रदाता को कॉन्टेंट पुलिस नहीं होना चाहिए

इंटरनेट अवसंरचना सेवाओं के प्रदाताओं पर ऑनलाइन कॉन्टेंट और भागीदारी को नियंत्रित करने में बड़ी भूमिका निभाने के लिए दबाव में हैं। कुछ अपने दम पर दखल देने का फैसला कर रहे हैं। यह एक खतरनाक प्रवृत्ति है जिसे अब समाप्त होना चाहिए।

हानिकारक भाषण समाप्त करने की लड़ाई में पूरी तरह से "स्टैक" की सूची में बुलाने की कुछ मामलों में समझ में आ सकती है, लेकिन यह अनपेक्षित परिणामों की एक श्रृंखला का नेतृत्व करेगा, विशेष रूप से कम शक्तिशाली उपयोगकर्ताओं के लिए। दुर्लभ अपवादों के विषय में, सरकारों को ऐसे हस्तक्षेपों की आवश्यकता नहीं होनी चाहिए और बुनियादी ढांचा कंपनियों को स्वेच्छा से हस्तक्षेप नहीं करना चाहिए

पृष्ठभूमि

उपयोगकर्ता और नीति निर्माता फेसबुक, ट्विटर या यूट्यूब जैसे प्लेटफॉर्म से बहुत परिचित हैं। लेकिन वे सेवाएं इंटरनेट नहीं हैं। वास्तव में, ऑनलाइन संचार और वाणिज्य सेवा प्रदाताओं की व्यापी श्रृंखला पर भी निर्भर करता है<}, जिसमें कॉमकास्ट, ऑरेंज, MTN, एयरटेल, मोविस्टार, या वोडाफोन जैसे ISPs और टेलकोस शामिल हैं; डोमेन नाम पंजीकरण जैसे Namecheap या GoDaddy(गोडैडी); Amazon Web Services (AWS){अमेज़ॅन वेब सर्विसेज (एडब्ल्यूएस)} जैसी सहायता सेवाएं<प्रमाण पत्र प्राधिकरण (जैसे आइए एन्क्रिप्ट करें), भुगतान प्रोसेसर जैसे PayPal और M-Pesa, ईमेल, मैसेजिंग सेवाएं, और अधिक। एक साथ लिया जाता है, इन प्रदाताओं को कभी-कभी "टेक स्टैक" कहा जाता है।

अधिकांश उपयोगकर्ता उन सभी अंतर्निहित बुनियादी ढांचा सेवाओं के बारे में सोचे बिना इंटरनेट का उपयोग करते हैं। लेकिन वे सेवाएं ऑनलाइन अभिव्यक्ति, गोपनीयता और सुरक्षा के लिए आवश्यक हैं। और जब ये प्रदाता-जिनमें से कई के पास उपयोगकर्ताओं के साथ कोई संपर्क नहीं है- कॉन्टेंट के आधार पर हस्तक्षेप करते हैं, तो उनके विकल्पों का मानवाधिकारों पर भारी प्रभाव पड़ सकता है जो निवारण के लिए मुश्किल या असंभव हो सकता है।

अभिव्यक्ति और गोपनीयता के लिए विशिष्ट नुकसान और जोखिम सेवा की प्रकृति के आधार पर भिन्न हो सकते हैं। लेकिन प्रत्येक बुनियादी ढांचा प्रदाता के लिए, निम्नलिखित चिंताओं का कुछ संयोजन लागू होगा। साथ में, वे शक्तिशाली रूप से प्रदर्शित करते हैं कि क्यों, दुर्लभ अपवादों के साथ, बुनियादी ढांचा प्रदाताओं को कॉन्टेंट पुलिसिंग से बाहर रहना चाहिए।

"द स्टैक" पर एक नोट

स्टैक कंप्यूटर विज्ञान और सॉफ्टवेयर इंजीनियरिंग से उधारित शब्द है, जिसका उपयोग एप्लिकेशन या उत्पाद बनाने के लिए संयोजन में उपयोग किए जाने वाले उपकरणों, प्रक्रियाओं, प्रोग्रामिंग भाषाओं और तंत्रों के संयोजन का वर्णन करने के लिए किया जाता है। इस संदर्भ में, हम इसका उपयोग इंटरनेट का वर्णन करने के लिए कर रहे हैं जैसा कि हम जानते हैं, सेवा प्रदाता, प्लेटफ़ॉर्म, प्रक्रियाएं और अलग अलग खिलाड़ियाँ जो आधुनिक वेब को संभव बनाते हैं।

टेक स्टैक में फेसबुक और ट्विटर जैसे उपयोगकर्ता-जनित सामग्री प्लेटफार्मों के साथ-साथ ऊपर उल्लिखित बुनियादी ढांचा प्रदाताओं की श्रृंखला शामिल है। सोशल मीडिया प्लेटफ़ॉर्म स्टैक के शीर्ष पर रहते हैं, जबकि आपके ISP प्रमुख आधारभूत बुनियादी सुविधा प्रदाता नीचे झूठ बोलते हैं, बिचौलियों की एक विस्तृत श्रृंखला के साथ- भुगतान प्रोसेसर सहित, और रजिस्ट्रार, दूसरों के बीच में बैठते हैं।

मानवाधिकारों के लिए जोखिम

1. अधिकांश बुनियादी सुविधाओं की सेवाएं, आवश्यक और अनुपातिक रूप से उनके हस्तक्षेप की प्रथाओं को रूपांतरित नहीं बना सकती हैं।

प्लेटफ़ॉर्म में अक्सर विभिन्न प्रकार के आधुनिकण विकल्पें. इसके विपरीत, कई बुनियादी ढांचा सेवाएं सटीक मानव अधिकार मानकों की मांग के साथ अपनी प्रतिक्रिया को लक्षित नहीं कर सकती हैं। ट्विटर कुछ खास ट्वीट्स को ब्लॉक करता है; अमेज़ॅन वेब सर्विसेज एक पूरी साइट या खाते की सेवा से इनकार करती है, जिसका मतलब है कि इनके हस्तक्षेप अनिवार्य रूप से कार्रवाई को प्रेरित करने वाले आपत्तिजनक भाषण से कहीं अधिक प्रभावित करते हैं। पूरे देश के लिए इंटरनेट को बाधित करने के लिए दूरसंचार सेवाओं का सरकारी अपहरण विशेष रूप से गंभीर है।

डोमेन स्तर पर भी गंभीर कार्यवाहियां होती हैं, जहां रजिस्ट्रार जो किसी वेबसाइट पर भाषण पर आपत्ति जताते हैं, वे केवल उस भाषण को लक्षित नहीं करते हैं, बल्कि पूरी साइट को निलंबित और/या अपंजीकृत करते हैं। उदाहरण के लिए, अनुच्छेद 19 ने "DNS दुरुपयोग)" के कई उदाहरणों का दस्तावेजीकरण किया है: असंतोष को दबाने के साधन के रूप में डोमेन नामों का निलंबन और पंजीकरण रद्द करना।

हम यहां कॉपीराइट संदर्भ से एक सबक ले सकते हैं, जहां एक ही दस्तावेज़ को लक्षित करने वाले उल्लंघन नोटिस के जवाब में पूरी साइट के संबंध में हमने डोमेन नाम रजिस्ट्रार और होस्टिंग प्रदाताओं को भी देखा है शट डाउन । कुछ सेवाओं के लिए ग्राहकों के साथ सीधे संवाद करना संभव हो सकता है जहां वे सामग्री के एक विशिष्ट टुकड़े के बारे में चिंतित हैं और अनुरोध करते हैं कि इसे नीचे ले जाया जाए। लेकिन अगर उस अनुरोध को अस्वीकार कर दिया जाता है, तो सेवा के पास अपने निपटान में पूरी तरह से हटाने का केवल कुंद साधन है। और कुछ सेवाओं में कॉन्टेंट के स्रोत के साथ सीधे संवाद करने का एक व्यवहार्य तरीका नहीं हो सकता है।

2. सार्थक नोटिस और अपील शायद ही कभी संभव है, खासकर कम शक्तिशाली के लिए।

मानवाधिकार मानकों और उचित प्रक्रिया सिद्धांतों की मांग है कि सेवा प्रदाता उपयोगकर्ताओं को सूचित करें कि उनका भाषण और / या खाता ऑफ़लाइन लिया गया है या होगा, और उपयोगकर्ताओं को निवारण की तलाश करने का अवसर प्रदान करता है। बुनियादी ढांचे के स्तर पर, इस तरह की सूचना और निवारण के अवसर असंभव हो सकते हैं। बुनियादी ढांचा सेवाएं अक्सर इंटरनेट उपयोगकर्ताओं के साथ सीधे संवाद करने में असमर्थ होती हैं क्योंकि सेवाओं का आमतौर पर स्पीकर या दर्शकों के साथ सीधे संबंध नहीं होता है। और प्लेटफ़ॉर्म-स्तरीय सामग्री होस्ट के विपरीत, जो हटाए गए पोस्ट के मूल स्थान पर एक व्याख्यात्मक सूचना छोड़ सकते हैं (एक अभ्यास में जिसे कभी-कभी "टॉम्बस्टोनिंग" कहा जाता है), बुनियादी ढांचे के प्रदाताओं में आमतौर पर भविष्य के उपयोगकर्ताओं को उन तरीकों < के बारे में सूचित करने की व्यावहारिक क्षमता की कमी होती है जिनमें प्रदाता ने कॉन्टेंट तक पहुंच में बाधा डाली है।

इस प्रकार, उदाहरण के लिए, यदि किसी उपयोगकर्ता को पता चलता है कि किसी मित्र द्वारा भेजा गया लिंक काम नहीं करता है, तो वे आसानी से नहीं जान सकते कि लिंक के साथ कोई समस्या थी या नहीं, क्या मालिक ने स्वेच्छा से साइट डाउन किया था, या क्या इसे अवरुद्ध कर दिया गया था। भुगतान प्रोसेसर पर निर्भर सेवा के उपयोगकर्ता भी सेवा को गायब करने के लिए चौंक सकते हैं क्योंकि, उनके लिए अनजान, प्रोसेसर ने उस सेवा के लिए भुगतान बंद कर दिया है। उदाहरण के लिए, अर्जेंटीना में, अदालत के आदेश के कारण उबर को रातोंरात काट दिया गया था, जिसके लिए सेवा के भुगतान को अवरुद्ध के लिए भुगतान प्रोसेसर की आवश्यकता थी।

उपयोगकर्ताओं को अनिवार्य रूप से स्पीकर से दर्शकों तक श्रृंखला में प्रत्येक सेवा के नियमों और शर्तों के लिए आयोजित किया जाता है, भले ही वे नहीं जानते कि वे सेवाएं क्या हैं या उनसे कैसे संपर्क करें। उल्लंघनों के संभावित परिणामों को देखते हुए, और पहले अदृश्य सेवाओं की अपील प्रक्रियाओं को नेविगेट करने की कठिनाई को देखते हुए (यह मानते हुए कि ऐसी प्रक्रिया पहले भी मौजूद है), कई उपयोगकर्ता पूरी तरह से विवादास्पद राय सांझा करने से बचेंगे। संबंधित रूप से, जहां किसी सेवा प्रदाता का स्पीकर या श्रोताओं से कोई संबंध नहीं है, किसी उपयोगकर्ता के भाषण के सूक्ष्म विश्लेषण की तुलना में व्यवसाय के लिए निष्कासन बहुत आसान और सस्ता होगा।

3. बुनियादी ढांचे के स्तर पर कॉन्टेंट -आधारित हस्तक्षेप संपार्श्विक क्षति का कारण बनता है जो कम शक्तिशाली समूहों को असमान रूप से नुकसान पहुंचाएगा।

सत्ता और प्रभाव वाले लोग अलोकप्रिय आवाजों और विचारों को दबाने के लिए अनिवार्य रूप से सेंसरशिप के लिए सभी प्रणालियों का शोषण करते हैं। दरअसल, बुनियादी ढांचे को अवरुद्ध करना सत्तावादी सरकारों का पसंदीदा उपकरण है। अक्टूबर 2019 में निरंतर सामाजिक अशांति की अवधि के दौरान, इक्वाडोर में इंटरनेट उपयोगकर्ताओं को बार-बार नेटवर्क ब्लॉकेज का सामना करना पड़ा। नाइजीरिया को ISPs पर महीनों के लिए ट्विटर पर प्रतिबंध लगाने की आवश्यकता पड़ी। यू.एस. प्रतिबंधों के एक व्यापक आवेदन के लिए धन्यवाद, AWS(एडब्ल्यूएस) ने अपनी सेवाओं से ईरानी उपयोगकर्ताओं को अवरुद्ध कर दिया है। क्लाउडफ्लेयर अस्वीकृत सेवा एक मास्टोडन उदाहरण के लिए जिसने अमेरिकी नियमों का हवाला देते हुए ऑस्ट्रेलिया में स्थित एक यौनकर्मी सामूहिक की मेजबानी की। और निश्चित रूप से कई देशों ने इंटरनेट को पूरी तरह से बंद कर दिया है।

इसके अलावा, यहां तक कि अच्छी तरह से इरादे वाले निर्णय लेने वाले नियमित रूप से हाशिए के लोगों के भाषण को कम आंकते हैं। प्लेटफ़ॉर्म स्तर पर, कॉन्टेंट मॉडरेशन में संलग्न कंपनियां लगातार हाशिए के समुदायों के खिलाफ पूर्वाग्रह को प्रतिबिंबित और सुदृढ़ करती हैं। उदाहरण भरपूर है: फेसबुक ने निर्णय लिया, #MeToo आंदोलन के उदय के बीच, "पुरुष कचरा हैं" कथन घृणित भाषण का गठन करता है; ट्विटर ने उत्पीड़न प्रावधानों का उपयोग करने का निर्णय लिया मिस्र के एक प्रमुख अत्याचार-विरोधी कार्यकर्ता के सत्यापित खाते को बंद करें; विभिन्न कॉन्टेंट मॉडरेशन निर्णयों ने गैर सफेद महिलाओं को रोका अपने मित्रों और अनुयायियों के साथ उनके द्वारा अनुभव की जाने वाली उत्पीड़न की कहानियों को साझा करने से; ट्विटर ने संदर्भ की परवाह किए बिना "क्वीर" शब्द वाले ट्वीट्स को आपत्तिजनक के रूप में चिह्नित करने का निर्णय लिया।

यहां तक कि जो मरीज प्रिस्क्रिप्शन की गई दवा नहीं खरीद सकते, वे भी प्रभावित होते हैं। हैशटैग में "ओपियोइड" शब्द पुलिस करने के प्रयास में और संबंधित शब्दों के उपयोग को, इंस्टाग्राम ने उन खातों को बंद कर दिया और प्रतिबंधित कर दिया जो ओपिओइड बेचने के लिए "दिखाई दिए"। एक परिणाम फ़ार्मेसीचेकर के खाते को बंद करना था, जो ऑनलाइन फ़ार्मेसी के बारे में सत्यापन और मूल्य जानकारी प्रदान करता है जो मरीजों और उनके देखभाल करने वालों को आयात के माध्यम से दवा खरीदने में मदद करते हैं, लेकिन दवा नहीं बेचते हैं।

यह सोचने का कोई कारण नहीं है कि बुनियादी ढाँचे की कंपनियाँ इन कॉल करने में प्लेटफार्म से बेहतर होंगी, और कई कारण यह सोचने के लिए हैं कि वे और भी बदतर होंगे।

4. राज्य और निजी अभिनेता किसी भी कॉन्टेंट-आधारित हस्तक्षेप मार्ग का अपहरण करने और उस पर नियंत्रण का विस्तार करने की कोशिश कर सकते हैं।

हस्तक्षेप के मार्ग, एक बार स्थापित होने के बाद, सार्वजनिक संवाद को नियंत्रित करने के लिए अतिरिक्त उपकरणों के साथ राज्य, राज्य प्रायोजित और निजी अभिनेताओं को प्रदान कर सकते हैं। एक बार प्रक्रियाओं और अभिव्यक्ति में हस्तक्षेप करने के उपकरणों का विकास या विस्तार हो जाने के बाद, कंपनियों को उनसे व्यापक रूप से लागू करने की मांगों में तेजी की उम्मीद हो सकती है। मंच स्तर पर, राज्य और राज्य-प्रायोजित अभिनेताओं के पास असहमति को शांत करने के लिए फ़्लैगिंग टूल को हथियारबंद कर दिया जाता है। और क्लाउडफ्लेयर, जो DDos हमलों से सुरक्षा सहित विभिन्न प्रकार की सेवाएं प्रदान करता है, रिपोर्ट्स कि, नव-नाजी साइट षड्यंत्र सिद्धांत साइट से सुरक्षा सेवाओं को वापस लेने के बाद, इसने सत्तावादी शासनों के अनुरोधों में नाटकीय वृद्धि देखी कि यह मानवाधिकार संगठनों के संबंध में भी ऐसा ही करता है।

कॉपीराइट के संदर्भ में, आलोचकों को चुप कराने के लिए निजी अभिनेता नियमित रूप से आसान निष्कासन प्रक्रियाओं का फायदा उठाते हैं। बुनियादी ढांचे के स्तर पर चीजें अलग होने की उम्मीद करने का कोई कारण नहीं है।

5. प्रतिस्पर्धा की कमी और स्विचिंग लागत कुछ कंपनियों को गलतियों या ठगी के लिए जिम्मेदार ठहराना कठिन या असंभव बना देती है।

जब कोई ISP किसी व्यक्तिगत उपयोगकर्ता के खाते को बंद करने का निर्णय लेता है, तो दुनिया के अधिकांश हिस्सों में, कोई अन्य प्रदाता उपलब्ध नहीं होता है: उपयोगकर्ता वास्तव में ऑफ़लाइन है। स्टैक की अन्य परतों पर, जैसे कि डोमेन नेम सिस्टम (DNS), कई ऐसे प्रदाता हैं जिनमें से चयन करना है—एक स्पीकर जिसका डोमेन नाम फ़्रीज़ है, अपनी वेबसाइट को कहीं और ले जा सकता है। लेकिन सिर्फ विकल्पों का अस्तित्व ही पर्याप्त नहीं है; हमें प्रदाताओं को बदलने की लागत और आसानी का मूल्यांकन करना चाहिए। शायद ही कोई सस्ता या आसान विकल्प हो। और कुछ स्थानों में, सरकारी कर्मचारी बुनियादी ढांचे की कंपनियों से निकटता से जुड़े हो सकते हैं; उदाहरण के लिए, केन्या सरकार के पास दूरसंचार कंपनी सफारीकॉम में 35% स्वामित्व है। और यहां तक कि जहां स्विच करना आसान है, यह मदद नहीं करेगा यदि स्टैक के एक निश्चित स्तर पर सभी प्रदाता समान कॉन्टेंट, स्पीकर और/या दृष्टिकोण को सेंसर करने के लिए चुनते हैं, या दबाव डालते हैं। आखिरकार, समस्या को जटिल किया जा सकता है जहां सेवा प्रदाता छोटे होते हैं और इसलिए, सरकारों और निजी अभिनेताओं के दबाव के लिए संभावित रूप से अधिक संवेदनशील होते हैं।

6. हस्तक्षेप की आवश्यकताएं प्रतिकूल हो सकती हैं।

ऑनलाइन भाषण को निशाना बनाने के लिए हस्तक्षेप करना वास्तव में उन लक्ष्यों को कमजोर कर सकता है जिन्हें इसे सेवा देनी चाहिए। उदाहरण के लिए, "चरमपंथी" सामग्री के निगरानी के पुलिस के प्रयासों से आतंकवाद और अन्य अत्याचारों का दस्तावेजीकरण करने के लिए पत्रकारों और मानवाधिकार रक्षकों द्वारा काम को अवरुद्ध या मिटा दिया गया है। किन्हीं खास देशों में इंटरनेट सेवाओं तक पहुंच को अवरुद्ध करने के दबाव में लोगों को सरकारी सेंसरशिप को बायपास करने और सटीक जानकारी तक पहुंचने में मदद करने के लिए अधिक प्रयास हैं।

7. बुनियादी ढांचे के स्तर पर सामग्री-आधारित हस्तक्षेप मौलिक इंटरनेट प्रोटोकॉल को कमजोर कर सकते हैं और सुरक्षा से समझौता कर सकते हैं।

कुछ इन्फ्रास्ट्रक्चर प्रोवाइडरों की सामग्री आधारित हस्तक्षेप, जैसे कि नेटवर्क पर डीप पैकेट इंस्पेक्शन (डीपीआई) घुसाया जाना या DNS प्रश्नों को अवरुद्ध करना इंटरनेट की वास्तुकला को गोपनीयता और सुरक्षा के नुकसान में पुनः आकार दे सकता है। उदाहरण के लिए, यदि DNS रिज़ॉल्वर के संचालकों ने केवल सामग्री के आधार पर कुछ डोमेन के लिए प्रश्नों को पुनर्निर्देशित करना शुरू करते हैं, तो यह DNS को दुर्भावनापूर्ण हस्तक्षेप के प्रति प्रतिरोधी बनाने के प्रयासों को बहुत जटिल करेगा, क्योंकि कंप्यूटर वेबसाइट स्पूफिंग के प्रयासों से "अच्छे" पुनर्निर्देशन को अलग नहीं कर सकते हैं। अगर प्रमाणपत्र प्राधिकारी निर्णय लेते हैं कि वे कुछ वेबसाइटों के लिए डिजिटल प्रमाणपत्र रद्द कर देंगे क्योंकि वे अपनी सामग्री पर आपत्ति करते हैं, तो "विश्वास की श्रृंखला" जिस पर बहुत अधिक इंटरनेट सुरक्षा निर्भर करती है, समझौता किया जाएगा इसके अलावा, खुले इंटरनेट> के एक प्रमुख डिज़ाइन सिद्धांत का उल्लंघन करके, बुनियादी ढांचे के स्तर के हस्तक्षेप इसके विखंडन में तेजी ला सकते हैं, क्योंकि लोग इस तरह के हस्तक्षेपों को बायपास करने के लिए नए बुनियादी ढांचे का निर्माण करते हैं और मौजूदा बुनियादी ढांचे के प्रदाताओं को परस्पर विरोधी नियमों का सामना करना पड़ता है और एक देश या किसी अन्य में अवरुद्ध होता है जिसके आधार पर वे पालन करते हैं।

8. असंगत नियम अनिवार्य हैं।

बुनियादी ढांचा प्रदाता, सभी सेवा प्रदाताओं की तरह, जो कई न्यायालयों में काम करते हैं, पहले से ही उन देशों के नियमों और मूल्यों के आधार पर परस्पर विरोधी आवश्यकताओं का सामना करते हैं जिनमें वे काम करते हैं। उन परस्पर विरोधी नियमों का पालन करना महंगा और कभी-कभी असंभव दोनों है। सामग्री पुलिसिंग में संलग्न होकर, वे दायित्वों के नए सेटों को आमंत्रित करते हैं जो नीचे तक एक लौकिक दौड़ का कारण बन सकते हैं, उदाहरण के लिए, सेवा में उतनी ही कॉन्टेंट को अवरुद्ध करना, जितना कि सबसे अधिक संवेदनशील अधिकार क्षेत्र को संतुष्ट करने के लिए आवश्यक है।

निष्कर्ष

इंटरनेट दुनिया भर के अरबों लोगों के लिए एक आवश्यक संसाधन है। हम इसका उपयोग संवाद करने, संगठित करने, विरोध करने, काम करने, सीखने, खरीदने और बेचने, सरकारी सेवाओं तक पहुंचने और बहुत कुछ करने के लिए करते हैं। यदि इंटरनेट को उस भूमिका को जारी रखना है, तो हमें इसे मज़बूत, साव्यय और सुरक्षित बनाने की आवश्यकता है। हमें बुनियादी ढांचा प्रदाताओं को उनके मुख्य मिशन पर ध्यान केंद्रित करने की आवश्यकता है: एक मज़बूत और साव्यय इंटरनेट का समर्थन करना। वह अभियान मानवाधिकारों की रक्षा करने की तुलना में कहीं अधिक महत्वपूर्ण है, बजाय कॉन्टेंट आधारित हस्तक्षेप प्रक्रियाओं को विकसित करने की कोशिश करने से जो लाजिमी तौर पर लाभ से अधिक नुकसान पहुंचाएगी।

हस्ताक्षरित

Access Now

American Civil Liberties Union (ACLU)

ARTICLE 19

ARTICLE 19 México y Centroamérica

ASEAN Youth Forum

Asociación por los Derechos Civiles (ADC)

Asociația pentru Tehnologie si Internet (ApTI)

Association for Progressive Communications (APC)

Bits of Freedom

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Chaos Computer Club (CCC)

Citizen D / Državljan D

Collaboration on International ICT Policy for East and Southern Africa (CIPESA)

Comun.al, Laboratorio de resiliencia digital

Data Privacy Brasil Research Association

Derechos Digitales - América Latina

Digitale Gesellschaft Schweiz (Switzerland)

Don’t Delete Art (DDA)

Electronic Frontier Foundation (EFF)

Epicenter.works - for digital rights

European Center for Not-for-Profit Law (ECNL)

European Digital Rights (EDRi)

Fight for the Future (FFTF)

Förderverein Informationstechnik und Gesellschaft (Fitug e.V.)

Foundation for Media Alternatives (FMA)

Freemuse

Fundación Huaira

Fundación InternetBolivia.org

Fundación Karisma

Fundación Vía Libre

Global Forum for Media Development (GFMD)

Hiperderecho

Homo Digitalis

Instituto Nupef

Instituto Panameño de Derecho y Nuevas Tecnologías (IPANDETEC)

Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

Instituto de Referência em Internet e Sociedade (IRIS)

Intervozes - Coletivo Brasil de Comunicação Social

IT-Pol Denmark

Kandoo

Masaar - Technology and Law Community

National Coalition Against Censorship (NCAC)

Open Knowledge Foundation

OpenMedia

Open Rights Group

Red en Defensa de los Derechos Digitales (R3D)

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

SeguDigital

SMEX

Southeast Asia Freedom of Expression Network (SAFEnet)

TAPOL

Taraaz

The Sex Workers Project of the Urban Justice Center

The Tor Project

The William Gomes Podcast

The Woodhull Freedom Foundation

Usuarios Digitales