February 2018

A NETWORK FOR ALL OF SAN FRANCISCO
NET NEUTRALITY, DIGITAL PRIVACY, & LOCAL CONTROL

San Francisco Blue Ribbon Panel on Municipal Fiber
Subcommittee on Privacy & Governance

Committee Chair San Francisco Mayor Mark E. Farrell
Subcommittee Chair Lisa Ho
Subcommittee Members Kit Walsh, Kevin Bankston, Professor Susan Freiwald, Asst. Professor Hao Yue, Professor Catherine Sandoval

The Municipal Fiber in San Francisco Reports

These reports will guide the City and County and San Francisco as it deploys a fiber-optic network citywide, in support of the City's longstanding effort to guarantee every single resident of San Francisco affordable, world-class high speed internet service.

This report addresses a question that could not be timelier given the Federal Communications Commission's December 2017 vote to repeal federal net neutrality and privacy authority: What security, privacy, and governance protocols are needed to ensure that Internet Service Providers (ISPs) operating on a city-wide fiber-optic facility deliver services that live up to San Francisco's values and expectations?

Like the panel reports that preceded this one, the Subcommittee's work on this topic will help frame consideration of how best to improve Internet connectivity across the City. Informed with the panel's input, San Francisco will better understand how to assess the policy challenges and opportunity costs it faces as the entire City decides whether to move forward with the overall project.

A NETWORK FOR ALL OF SAN FRANCISCO

Blue Ribbon Subcommittee on Privacy & Governance

Introduction

This document offers a high-level set of recommendations to operate a new, locally owned and controlled network across the City and County of San Francisco (the "City").

Background. After assessing the status quo of broadband access in San Francisco, City leadership set forth policy goals to address gaps in Internet quality, choice between providers, and equitable access. [#] The public broadband, "open-access" approach the City formally proposed will allow San Francisco to leverage its authority as the owner of a new network and ensure the network serves as a community asset. [#] The City should build and operate such a network in accordance with the following recommendations.

Recommendations. This report recommends policies and technical practices to protect deeply held values of San Francisco residents. San Francisco deserves an **open access network** that requires private operators to provide residents **equal access to all lawful content**; enforces **mandates for privacy and consent**; and ensures robust procedures to **protect residents from overreaching, extra-legal requests.**

Next Steps. The sections that follow provide details and additional recommendations, but to chart the path forward from here, we also propose a community-driven process to establish final determinations about how the City will exercise oversight over the entire network.

Ensuring Open Access

San Francisco should proceed with an open access approach: a city-wide fiber network that is owned by the City but leased to private ISPs in order to promote competition and consumer choice. [1]

Open Access Promotes Market Competition. An open access fiber network will improve affordable Internet service across the City. The driving force is familiar: customer choice drives companies to compete on service, cost, and consumer protections. Open access models work by lowering the switching costs for customers and reducing the investment costs for new providers to enter the market. Users can discourage abusive practices by switching to a provider that better suits them. Competition improves the incentive to provide high speed, reliable service at an affordable cost: as users will have choices between service providers, rather than being powerless to escape an ISP that is unreliable or provides low quality service.

Protecting Free Expression and Net Neutrality

Freedom of Expression

No one should have the power to decide what you may or may not say online: not the City or your ISP. The same goes for what you read: you should be in control of what news sources you read and how you want to educate yourself and your family.

The Internet has been a powerful tool for people to publish and learn without needing a professional publisher or other institution. Social movements rely on the Internet to coordinate action, discuss the issues, and build community.

But this beneficial state of affairs takes work to maintain, because the Internet also creates dangerous new opportunities for ISPs or governments to control access to knowledge and opportunities to speak. For instance, an ISP has the technological capability to block access to websites of its choosing, to insert its own content in place of content you seek or transmit, or even filter out certain content, or enrich itself by charging your favorite video provider extra money just to reach you.

San Francisco can protect its residents' access to information and freedom of speech by ensuring it and the ISPs that operate over its network do not unduly interfere with information passing over the fiber network.

Network Neutrality

ISPs should treat all data that travels over their networks fairly, without discrimination in favor of particular apps, sites, or services. This is the principle known as Net Neutrality, and it is a principle that must be upheld to protect the Internet's role as a force for empowering its users rather than for consolidating power in the hands of private companies that own or operate the pipes. With the federal government moving away from protections for Net Neutrality, it falls on state and local government to protect against unfair data discrimination that stifles speech, learning, and the economy.

Net Neutrality is a principle that's faced many threats over the years, such as ISPs forging data to tamper with certain kinds of traffic or slowing down or even outright blocking protocols or applications.

Net Neutrality can be protected by a few clear, important rules that should apply to ISPs operating over the City's fiber infrastructure. If the City adopts clear rules following the model provided by the FCC in 2015, it can help to ensure the Internet will continue to serve as a vibrant space open for all voices.

1. **No blocking** of particular sites, content, or applications. You may visit any page you like, say what you like, and attach the device of your choice without interference by the ISP.

2. **No throttling (slowing down)** sites, content, or applications.

3. **No 'paid prioritization'**– an ISP cannot favor its own content or content of its commercial partners. Nor can an ISP favor any other content in exchange for any type of compensation or consideration. This rule is important because it prevents the creation of fast and slow lanes, which may favor commercial content and drown out educational and expressive speech. It also keeps ISPs from picking winners and losers online.

These are simple, understandable rules that mitigate the proven harms of data discrimination.[1] Some such harms include blocking of content – such as AT&T's blocking of the Apple FaceTime app or Comcast's blocking of peer-to-peer technology – as well as throttling (common on mobile networks but also infamously used by Comcast to put pressure on Netflix). [2] [3] [4] [5]. While big companies like Apple and Netflix can afford to pay off ISPs, it's important to protect the small companies that might one day unseat today's giants, by protecting Net Neutrality.

The City can also ensure via transparency rules that ISPs provide accurate information about network practices, pricing, and network speeds, so that customers are not misinformed. Additionally, San Francisco should oversee ISP practices on its network as they evolve to determine if additional clear rules are appropriate to introduce to protect residents and meet the City's longstanding policy goals.

Protecting Security and Privacy?

An ISP's privileged role as a gatekeeper between its users and every other person or service on the Internet doesn't just raise free expression concerns; it raises privacy concerns as well. Every email, web page, picture, video, audio file, social network post, and instant message – every personal communication, every business communication, any Internet communication no matter how sensitive – is transmitted through the ISP's facilities. That means the ISP, or anyone who can gain access to its network whether by hacking into the ISP's facilities or making a legal demand to the ISP can obtain those communications unless there are adequate safeguards. Even users and websites using encryption to scramble the contents of their communications still generate a wealth of other non-content information that is accessible regardless of encryption (comparable to what you'd find on a detailed phone bill) which can reveal where and when you are going online, who you're communicating with, what web pages you are visiting, what apps you're using, and more. Even security monitoring can be invasive if data is misused for surveillance.

[1] San Francisco should adopt these rules as stated and defined by the 2015 Open Internet Order.

Suffice to say, an ISP has uniquely powerful ability to see into the private online lives of its users, and access to such a broad range of revealing information is ripe for abuse absent strong privacy protections. [6] [7] Therefore, it is critical that San Francisco develop robust policies that safeguard both privacy and security to ensure that the residents and businesses using its network are protected--whether against outside attackers trying to hack their data, service providers seeking to commercially exploit their data unfairly, or overreaching legal demands by government investigators or civil litigants.

Protecting Network Security Against Outside Attackers

Confidentiality, Integrity, Availability. Network Security refers to the policies and practices adopted to protect the assets of a network, including the infrastructure, software, and data. A well-known model for network security is the C-I-A triad, which stands for Confidentiality, Integrity, and Availability.

- **Confidentia**lity: Network assets are not made available or disclosed to unauthorized individuals.
- **Integrity:** Network assets, especially data, are not modified or deleted except as authorized.
- **Availability:** Network assets must be available to authorized parties when needed.

Network Security Measures. Common network security measures to achieve the C-I-A triad include encryption, firewalls, malware protection, Intrusion Detection Systems, etc. Encryption is the conversion of information or data into another form that is difficult for unauthorized individuals to decode. Firewalls are network security devices and software that monitor incoming and outgoing network traffic and decide whether to allow or block specific traffic based on predetermined security rules. Malware protection can detect and remove malicious software in computers and networks, such as viruses, worms, and Trojans. Intrusion Detection Systems are devices and software that monitor a network for possible security breaches and notify network administrators when breaches occur. ISPs should provide, support, and/or encourage the use of such security measures as appropriate.

Transparent Governance. In the face of increasingly intense and sophisticated attacks, service providers and consumers alike must continually improve and evolve their information security protections. Last decade's security measures would be insufficient in today's threat environment, just as today's protections will be inadequate against the attacks of the future. This calls for transparent and inclusive governance to ensure policies and practices evolve to remain effective while staying in alignment with the community's values.

How is "Privacy" Different From "Network Security"?

Network Security is about making sure the network works as intended, without intrusion or disruption. Privacy requires us to think about how the network is intended to work: who has access to private information about Internet users and how they are allowed to use that information. [8]

Protecting Consumer Privacy

As intermediaries between their users and the rest of the Internet, ISPs have access to a vast amount of private data, detailing not only when and how their customers use the Internet, but also much of the content of their private communications. Customers have little choice but to transmit this information over their ISP’s facilities in order to access the Internet. This leaves their data open to potential exploitation by the ISP for purposes other than providing Internet service. For example, an ISP might want to sell data about its users’ private online habits, or use that sensitive information to serve targeted advertising. Indeed, absent strong privacy protections dictating otherwise, a provider might require a user gives consent to such privacy-invasive practices in exchange for accessing the Internet at all -- or may charge an extra fee to users who refuse to consent.

Recognizing these risks to Internet users’ privacy, the FCC established new privacy rules in October 2016 that gave consumers greater control over their ISPs’ use and sharing of their personal information.[9] Those rules were quickly rolled back in early 2017 by the new Congress and President. [10] However, responding to broad public opposition to that privacy rollback, elected leaders in California sought to fill the gap by imposing new broadband privacy rules of their own. [11] Inspired by the FCC’s rule, Assembly Bill 375 sought to ensure that California consumers have meaningful choices when it comes to how their ISPs use, disclose, and sell their data. [12]

Although the bill has been ordered to inactive status as of September of 2017, the consumer protections that would be established by the version of the legislation as amended by the California Senate on June 19, 2017 constitute a strong model approach to broadband privacy that San Francisco should adopt as policy for providers operating on its network. [13] Among other critical protections, the bill would require -- and San Francisco should require -- that ISPs adhere to the following rules:

- As a general matter, ISPs cannot use, disclose, sell, or permit access to a customer’s personal information (which includes financial and health information as well as web browsing and app usage history), unless the customer provides prior opt-in consent.

- ISPs cannot refuse to serve or otherwise penalize in any way those customers who choose not to give consent. Similarly, ISPs cannot offer a customer a discount or benefit, not penalize a customer, based on the customer’s consent decision, thereby preventing “pay for privacy” schemes that would disadvantage lower-income customers.

- ISPs must give customers a mechanism for opting out of any use of their data to advertise any “communications-related” services.

- ISPs must get affirmative opt-in consent for use and disclosure of “de-identified” data.

These vital protections would go a long way toward ensuring the digital privacy of San Francisco residents, while setting a strong example for other municipalities across the nation as they consider how best to protect the privacy of their own residents.

Privacy & Civil Liberties: Protecting Against Overreaching Legal Requests

San Francisco should establish policies that require any ISP operating on its network to protect privacy in the face of legal demands for data. Under the Electronic Communications Privacy Act, or ECPA, ISPs may not disclose the contents of users' communications in response to legal process initiated by private parties rather than government agents. [14] For information not covered by ECPA, ISPs should not disclose such information to private parties unless compelled to do so by legal process.

When California government entities demand access to communications and related data, California law provides broad protection under the recently enacted California Electronic Communications Privacy Act (CalECPA). [15] Whether the demands pertain to communications as they happen or to stored data, CalECPA requires government entities to obtain a warrant based on probable cause that is limited in scope to only relevant information. Users must be told about the investigation, at some point, and they may challenge it in court for not following the dictates of CalECPA.

ECPA provides fewer protections to users for investigations pursued by federal agents, but users will have stronger claims to constitutional protections under the Fourth Amendment if an ISP acts as a mere intermediary. That means that San Francisco should require that ISPs adopt policies under which they disclaim any right to access, inspect or monitor their users' communications information. [16] ISPs should access their users' communications only for the limited purpose of ensuring adequate service, and they should further disclaim any ability to consent to the disclosure of communications and related information. Further, when required to disclose user data to federal investigators, ISPs should notify their customers unless ordered not to do so, and they should challenge any order that seems unjustified or overly broad. [17]

Encouraging Encryption

Encryption technology is one of the key methods for protecting data online, which allows data to be safely stored and transferred across a network. Encryption can convert electronic data into another form, called ciphertext, which cannot be understood by anyone except authorized parties. By making data and information unreadable, encryption could make it more difficult for unauthorized individuals to access that data, even if a network is accessed or compromised. Encryption is also effective in protecting sensitive data, including personal information for individuals, which can ensure privacy of customers and reduce opportunities for surveillance by both attackers and ISPs.

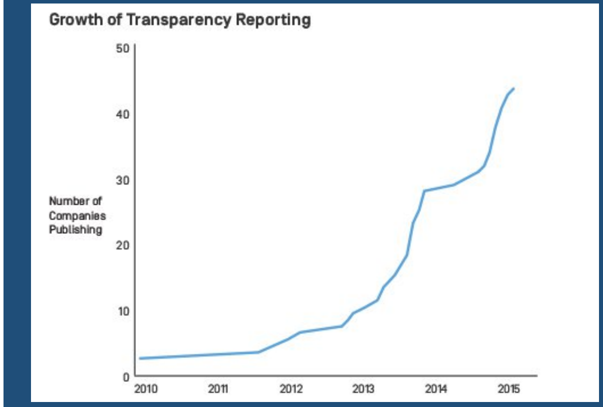
By encouraging the use of encryption over its network, San Francisco will ensure technical protections are in place that overlap in function and align in purpose with the legal and regulatory protections we have recommended throughout this report. Exercising its oversight authority as owner of the network, San Francisco should make clear that ISPs leasing the network must not block or otherwise thwart their customers' uses of encryption technology. In its capacity as a source of community education, the City should likewise include encryption training as a standard component of any digital literacy education funded through lease revenue generated by the network.

Transparency Reporting Around Legal Requests

Another key mechanism for public accountability and education around legal demands for user data is the practice of "transparency reporting." [18] Transparency reporting has recently become a standard practice amongst online providers in the U.S. and is increasingly prevalent around the world. [19] From telecom giants like Verizon and Comcast to smaller providers like Sonic.net or University of California, Berkeley, ISPs are increasingly issuing--and are expected to issue--transparency reports. San Francisco's network and the providers that offer service over it should be no different, and the subcommittee strongly urges that transparency reporting be a mandatory feature of San Francisco's broadband future.

Although there is a great deal of diversity in terms of the format and content of different providers' transparency reports, all are at their most basic a summary of how many and what kind of legal requests were received in a particular time period, often with additional details around what types of information was requested, how many of the demands resulted in disclosure of data, and more. New America's Open Technology Institute (OTI) and Harvard's Berkman Klein Center for Internet & Society recently completed an extensive research survey of the current best practices around transparency reporting on government data requests, isolating examples of where companies are doing a good job of clearly defining and counting requests, and are providing useful additional features to place that data in context. [20] Those best practices have been consolidated into a standardized transparency reporting template and guidebook for providers seeking to develop and publish a transparency report for the first time. [21] We recommend that providers seek to adhere to the best practices identified there in regard to issuing regular reports on legal demands for disclosure of data. Also, and consistent with the free expression principles detailed above, we similarly urge that providers follow the increasingly common practice of regularly publishing transparency data detailing legal demands for the takedown or blocking of particular content. [22]

New America's Open Technology Institute: "Getting Internet Companies To Do The Right Thing," Case Study #3: Transparency



In this case study (link), panel member and OTI Director Kevin Bankston and co-authors at Harvard's Berkman Klein Center explain (link): "*publishing aggregate data about government requests for user data, government demands to remove content, and intellectual property-related takedowns, transparency reports offer companies a public-facing opportunity to showcase their values and commitments to protecting user rights.*"

Providing for Ongoing Community Engagement in Governance

This report has only begun to ask the hard questions—and propose thoughtful answers—about how San Francisco's municipal broadband network should be governed and how the privacy of residents who use the network should be protected. This subcommittee's final recommendation therefore focuses on the need to continue the work that we have begun, by building long-term governance structures and processes that ensure ongoing engagement by the Mayor's office, the Board of Supervisors, and most especially the community itself in future decision-making around this crucial resource. When it comes to digital technology, the only constant is change, and the City and its residents will continually need to make new decisions about how the network will grow, how it will be used, what new technologies will or won't be integrated into it, and how the network's policies and privacy practices will change as the network itself changes.

Thankfully, several cities have recently been innovating in the arena of tech and privacy governance, and we urge the City to look to these examples to begin formulating its own plans. Most advanced in this work is the City of Seattle. In 2015, Seattle designed a privacy program for city employees working with personal information. That Seattle Privacy Program, developed with the assistance of an expert Privacy Advisory Committee, resulted in the development of a clear city-wide privacy policy setting forth requirements regarding Seattle's handling of data—including a process to review projects with privacy impacts and guidance on how to mitigate those impacts—consistent with a basic set of privacy principles and a privacy statement outlining the city's obligations. [23] [24]

City-level innovations around governance of policing and surveillance technology should provide useful models for governance of San Francisco's network. Seattle again has been a leader in this area, as the first city to require council approval prior to city departments purchasing surveillance tech. Further, the Seattle city council must provide an assessment of privacy impact and measures to mitigate the impact prior to deployment of that equipment. [25] Seattle updated their ordinance in 2017 to increase the required level of community outreach in the approval process. [26] In particular, departments seeking approval must now ensure *residents* are informed about the new technology, and the council must consult a community advisory group.

Cities in California including Oakland and Santa Clara have passed ordinances to ensure greater transparency and better decision-making around procurement and use of new surveillance technologies. [27] [28] We strongly urge San Francisco to join in this trend and expand it to include not just surveillance technologies but also municipal broadband-related technologies, which—as this report described—also greatly impact privacy. San Francisco residents must continue to play a central role in deciding what new technologies the City should procure and deploy and what policies should govern them.

Page 2/4

[1] Community Networks: Open Access, http://bit.ly/2Bv3czj

[2] Free Press, “AT&T Blocking FaceTime,” http://bit.ly/2BM6o6s

Page 4

[3] Electronic Frontier Foundation, “Comcast Caught Again,” Feb. 28, 2008, http://bit.ly/2p6gwnV

[4] Raniyah Bassel Tayeon, “Throttling on Mobile Networks is a Sign of Things to Come, Unless We Save Net Neutrality Now,” Electronic Frontier Foundation July 27, 2017, http://bit.ly/2paH7Ac

Page 5

[5] Cecilia King, “Netflix Strikes Deal to Pay Comcast to Ensure Online Videos Are Streamed Smoothly,” Feb. 23, 2014, http://wapo.st/2kUxFeY

[6] Upturn, “What ISPs Can See: Clarifying the technical landscape of the broadband privacy debate,” March 2016, http://bit.ly/2y8SIDT

[7] New America’s Open Technology Institute [OTI], “The FCC’s Role in Protecting Broadband Privacy: An Explainer,” Jan. 2016, http://bit.ly/2ySrT45

[8] “ UC Berkeley Privacy and Information Security Initiative,” Jan. 2013, http://bit.ly/2ol60Wo | Office of the Executive Vice Chancellor, University of California, Feb. 28, 2013, http://bit.ly/2kBp2qs

Page 6

[9] FCC, “Report and Order In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,” adopted Oct. 27, 2016, http://bit.ly/2zULrVw

[10] S.J.Res.34 - "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,” Public Law No: 115-22 on 04/03/2017, http://bit.ly/2zU7KLd

[11] Matthew Yglesias, “Republicans’ rollback of broadband privacy is hideously, unpopular,” Vox, Apr. 4, 2017, http://bit.ly/2zKcwtH

[12] James K. Willcox, “States Push Their Own Internet Privacy Rules,” Consumer Reports, Apr. 20, 2017, http://bit.ly/2yQRnBe

Page 7

[13] California Assembly Bill No. 375 (2017) as amended in Senate on Jun. 19, 2017, http://bit.ly/2Bwuo0E

[14] Federal law does not permit disclosure in response to civil demands. See 18 U.S. 2702, http://bit.ly/2BNCpex

[15] Cal. Penal Code sections 1546, 1546.1, 1546.2 and 1546.4

[16] *U.S. v. Warshak* (6th Cir 2010), http://bit.ly/2Bipccy

Page 8

[17] U.S. DOJ Memo, Oct 19, 2017, http://bit.ly/2BvnBV3

[18] New America’s Open Technology Institute (OTI), “Getting Internet Companies To Do The Right Thing” Feb. 9, 2017, http://bit.ly/2paICP2

[19] Access Now, “Transparency Reporting Index,” Fall 2016, http://bit.ly/2yWX28K

[20] OTI/Berkman Klein Center for Internet & Society at Harvard University, “Transparency Reporting Toolkit,” Mar 2016, http://bit.ly/2kXPmun

[21] OTI/Berkman Klein, “Transparency Reporting Toolkit” Dec. 2016, http://bit.ly/2kXPmun | Dec. 2016, http://bit.ly/2Ds4SHh

[22] E.g., Transparency Reports by Twitter (http://bit.ly/2lmmtv5), Microsoft (http://bit.ly/2gOHkGb), and Google (http://bit.ly/2lq4vYT).

Page 9

[23] Seattle.gov: Seattle Information Technology, “Privacy Advisory Committee,” http://bit.ly/2zJKcI4

[24] Seattle.gov: Seattle Information Technology, “Privacy,” http://bit.ly/2hgf787

[25] Seattle, WA Ordinance 12412 (2013) http://bit.ly/2y8iOXL

[26] Seattle.gov: Council Connection, “Council Approves Strongest-in-Nation Surveillance Technology Transparency Ordinance,” Jul. 31, 2017, http://bit.ly/2zUWCxI

[27] City of Oakland, “Privacy Advisory Commission,” http://bit.ly/2iaoMMP

[28] Santa Clara County, Ordinance Division A40-2 (2017), http://bit.ly/2y9GYBl

Image Credits

Icon on page 1 (and throughout) made by Roundicons

All images available through www.flaticon.com