Defending Privacy In The Surveillance State And Fragmenting Internet

John P. Ruehl – Source: Independent Media Institute

05-20-2024 ~ *Governments and private entities have steadily eroded privacy on the internet. The trend toward internet functions centralizing within national borders and fragmenting internationally reinforces the need to safeguard both openness and security in cyberspace.*

Following the reapproval of the Foreign Intelligence Surveillance Act (FISA) on April 20, 2024, Senate Majority Leader Chuck Schumer proudly declared that "bipartisanship has prevailed here in the Senate." Despite the increasing rarity of bipartisanship in recent years, support for government surveillance continues to unite large majorities across party lines. Established in 1978, FISA allows government surveillance and data collection of individuals suspected of espionage or terrorism within the U.S., marking one of the many mechanisms aiming to ensure total federal oversight of communications.

Governments ranging from democracies to dictatorships, socialist to capitalist have all developed policies and bureaucracies for maximum data collection and mass surveillance as their populations become digitized. The centralized nature of modern communications grids facilitates many forms of surveillance. As internet services centralize domestically and the internet fragments internationally, countering government and private sector abuse of surveillance or developing alternative systems will require steady public pressure and some ingenuity to attain real enforcement.

One of the takeaways that a review of the history of modern surveillance, from the early days of the telephone to so-called privacy apps like Signal, tells us is that efforts to escape, undermine, and subvert the surveillance efforts of governments tend to be counterproductive. They are often originated by states themselves as part of a dialectic process that enables more comprehensive surveillance in a series of stages or just produces greater surveillance infrastructure in response to the attempt to develop alternative communications systems.

In the pre-internet era, authorities would tap into telegraph and later telephone lines to intercept communications, often requiring access to the physical infrastructure of the networks. Mail sent by post could meanwhile be intercepted and opened. As communication systems evolved, so too did government techniques to surveil them. The switch from copper wire phone systems to fiber optic cables and the spread of the internet initially threatened the NSA's ability to monitor communications, for example, until the Communications Assistance for Law Enforcement Act (CALEA) in 1994. Communications companies were required to build back doors for the NSA to monitor remotely, while the NSA also clandestinely worked on developing technologies to monitor communications.

U.S. domestic surveillance powers have been routinely updated during the 21st Century, including the enactment of the 2001 PATRIOT Act, the 2015 Cybersecurity Information Sharing Act (CISA), and the 2018 FISA reauthorization. The 2013 Snowden Leaks revealed the NSA asked for funding to "insert vulnerabilities into commercial encryption systems", and it is constantly pushing for backdoors into encryption software to access communications and devices. Major mobile carriers acknowledge the inclusion of preinstalled surveillance and data mining technology in devices supported by Google, Apple, and Microsoft, while the NSA's PRISM program extracts data from all major technology companies with or without their consent.

U.S. companies primarily cooperate with the U.S. government under the banner of "surveillance capitalism," allowing them to capitalize on their data and surveillance capabilities both for government and private endeavors. Similar to other countries, most of the U.S. internet traffic now flows through a handful of large entities rather than numerous smaller ones. Furthermore, U.S. user data is also more available to the private sector compared to that of EU citizens, with companies like Facebook and Google even compiling dossiers on non-users to enhance targeted advertising.

In addition to ad monetization, lax privacy laws also play a role in security. Established in 1976, the third-party doctrine allows U.S. law enforcement to access user data without a warrant. The Ring video system, acquired by Amazon in 2018, created hundreds of partnerships with U.S. police departments to help them gain access to user recordings, while numerous other companies actively provide law enforcement agencies with access to user data.

The issue extends beyond monetization and law enforcement. Political actors have recognized the potential of data to shape politics. In 2018, Facebook faced scrutiny when it was revealed that private company Cambridge Analytica was permitted to access user data and target them with political ads to influence their voting behavior. Moreover, anti-abortion groups have caused controversy by using location data to send ads to those who visited Planned Parenthood centers.

Of similar concern is the abuse of data by employees. In 2017, reports surfaced of employees of Ring doorbell company spying on female users, while Amazon's Alexa retained recordings of children long after parents requested their deletion. Hackers have also accessed user data and feeds of Ring customer cameras across the U.S.

Alongside extensive domestic surveillance and data collection methods, the expansion of the internet in the 1990s led to a surge in global U.S. surveillance and data collection capabilities. Despite the promotion of a "global multi-stakeholder model of internet governance", U.S.-based Organizations like the Internet Corporation for Assigned Names and Numbers (ICANN), Internet Engineering Task Force (IETF), and Worldwide Web Consortium (W3C), allowed Washington considerable control over the governance, standards-setting, and the activities of major internet actors. While these advantages for Washington may have declined since the 1990s, the rise of Big Tech and other factors guarantee the U.S. ongoing influence over much of the internet.

The disclosure of ECHELON in the 1990s exposed a global signals intelligence (SIGINT) network operated by the U.S., UK, Canada, Australia, and New Zealand

(Five Eyes), while the Snowden leaks in 2013 uncovered further aspects of the surveillance alliance. Significant data sharing also occurs between the U.S. and European countries, often facilitated through organizations like NATO.

The 2022 interception of a British citizen's Snapchat message about a potential plane bombing, leading to the escorting of the plane by the Spanish air force, demonstrates strong Western data and surveillance collaboration. Multilateral efforts are supplemented by national measures like France's Intelligence Act and the UK's "Snooper's Charter."

Nonetheless, the U.S.-led internet faces mounting challenges as various blocs and countries impose restrictions and tighten control over their networks. The Snowden leaks exposed the ability of the Five Eyes to circumvent their domestic spy laws and even target high-profile officials like the German chancellor. Partly in response to the leaks, the EU introduced the General Data Protection Regulation (GDPR) in 2018 to limit data intrusion by foreign states and corporations and improve regulations on data collection.

Countries more hostile to Washington are also asserting greater autonomy over their data and communications networks, leading to more apparent cracks in the global internet. The Russian government's takeover of Russian social media site VKontakte in 2014 and increasing pressure on Telegram and Yandex in recent years have helped reinforce the Kremlin's concept of a "sovereign internet." The Russian government has conducted several trial runs of disconnecting the country from the global internet, while its efforts to centralize control and quell dissident opinion have intensified since the launch of the war in Ukraine, including blocking access to Western sites.

Moscow has also been re-establishing surveillance and data-sharing agreements with Central Asian states since the Soviet collapse, using these arrangements to target Russians who fled abroad after the invasion of Ukraine. China's autonomy from the U.S.-dominated internet infrastructure is more advanced, and in Central Asia and other regions, Chinese companies vie with Russian counterparts for the export of surveillance and data collection technologies.

Notably, Western companies have played an influential role in assisting authoritarian governments to enhance their communications control and reduce dependence on U.S.-led internet infrastructure. U.S. corporations like Cisco helped build the “Great Firewall of China” and domestic surveillance capabilities, while Palantir assisted the United Arab Emirates. Nokia meanwhile contributed to Russia’s development of its System for Operative Investigative Activities (SORM), which has also been replicated across Central Asia.

In response to concerns over decreasing privacy from government surveillance and private sector data collection, various initiatives have emerged in the decades since the internet appeared. These range from underground forums to marketplaces for illicit goods and servers, as well as blockchain technology, a decentralized method of storing and sharing data through computers. Search engines like DuckDuckGo position themselves as untraceable, while virtual private networks (VPNs) encrypt internet traffic to provide users with anonymity and data security. Tor, a software that reroutes and encrypts internet traffic through several to protect user identities, went public in 2002. A follow-up app, Signal is internationally believed to be a viable encrypted and private messaging platform.

Together, these components constitute what users are told is the Dark Web or darknet, an obscured part of the internet that is perceived as a means to evade government surveillance and control. But many of them have their roots in the same surveillance world that their marketers claim to be opposed to. Meanwhile, DuckDuckGo’s privacy has been questioned, VPNs can be compromised, and flaws in Tor’s code are found regularly. Early U.S. government involvement and funding in both Tor and Signal suggest they are less secure than promoted. Tor was originally developed by the U.S. Naval Research Laboratory in the mid-1990s before it went public, while Signal was partly funded by the government-sponsored Open Technology Fund (OTF), which has ties to the U.S. intelligence community.

The appointment of Katherine Maher to the chairman of Signal’s board in 2023, who previously worked for the National Democratic Institute and Foreign Affairs Policy Board, has also raised questions about the app’s security. Other anti-surveillance projects developed partly by the OTF, including Open Whisper Systems, CryptoCat, LEAP, and GlobaLeaks, have also had their authenticity questioned.

Dark Web-affiliated systems are also used by states. Russian authorities began cracking down on VPN services, Tor, and other services just before the war in

Ukraine, but a year later, they cautiously permitted the expansion of these closely monitored channels to circumvent sanctions. The Iranian government also has a long history of using the dark web to more effectively evade U.S. oversight, while also striving to prevent its citizens from using it to undermine state authority. Even the CIA has developed its own Tor website for communication.

To avoid the dilemma of choosing between a government-monitored internet in collaboration with Big Tech and a lawless Dark Web of dubious anonymity, a middle ground termed Web 3.0 has emerged. Characterized by buzzwords like decentralization and blockchain technology, its proponents seek a more community-driven and peer-to-peer internet landscape with less surveillance and control by the current arbiters of the internet.

However, without true anonymity, these transparency efforts will make surveillance easier. Governments not only develop national and international communication systems but also support private initiatives and those developed by Academia to maintain control over all potential communications systems, including Web 3.0. If certain systems emerge that threaten government surveillance measures, they are either shut down, like the Silk Road, or compromised by various methods including operatives in both U.S. and foreign companies. Instead, Web 3.0 may be more useful in preserving the more open and connected aspect of the internet, though it will still be widely monitored.

Computer hardware and operating systems enable these apps to function inside devices that permit an overlay of surveillance on user activity, no matter the alleged privacy capabilities promised to users. The U.S., Australia, and other countries' efforts to ban Chinese-made Huawei devices highlight the ease of data collection and surveillance through such technologies, revealing similar capabilities in U.S.-made devices, despite the alleged security provided by privacy apps and other measures. The escalating rivalry between the U.S. and China in developing massive new undersea internet cables shows the intensifying efforts of rival blocs to secure their own communications and surveil others.

Without the ability to create an alternative system not dominated by governments and Big Tech, stronger public oversight over their surveillance and data collection methods is essential for personal privacy. The 34 Senators who voted against FISA's reauthorization in April demonstrated bipartisan support exists for reducing the government's surveillance and data collection powers, while 15 U.S.

states have so far adopted stronger data privacy laws for consumers in recent years.

Creating a clear and enforceable punishment system for both government agencies and private companies for data and surveillance abuse will be essential for any attempt to establish greater privacy safeguards. Increasing public awareness of the overt surveillance capabilities of devices and apps, even amidst the massive growth of the privacy protection industry, is a quick way to advance this cause.

By John P. Ruehl

Author Bio: John P. Ruehl is an Australian-American journalist living in Washington, D.C., and a world affairs correspondent for the Independent Media Institute. He is a contributing editor to Strategic Policy and a contributor to several other foreign affairs publications. His book, *Budget Superpower: How Russia Challenges the West With an Economy Smaller Than Texas'*, was published in December 2022.

Credit Line: This article was produced by Economy for All, a project of the Independent Media Institute.