The Wild West is Less Wild Than You Think:
The Role of Lawful Intercept in Safeguarding Data Collection

As the world becomes increasingly connected, network traffic analysis has proven invaluable. Network traffic analysis relies on deep packet inspection ("DPI") to monitor and troubleshoot the performance and security of both the network, applications, and services running over the network. DPI is highly effective at determining baseline application behavior, analyzing network usage, troubleshooting network performance, and looking for security threats. This description barely scratches the utility of this technology.

When network traffic analysis is used responsibly by IT professionals, it can be an invaluable tool. Some remain suspicious, however, that in the hands of less-than-scrupulous governments or ethically-challenged corporations driven by profit motives, DPI could be a dangerous tool.

While DPI holds the potential for misuse, the beneficial aspects of network traffic analysis is undeniable. For that reason, legal safeguards have been put in place that dictate the lawful collection of this data. Court orders must be obtained to gather said information. In this paper, Tim O'Neill, an independent network and communications technology expert and Advisory Board Member of the DPI Consortium, shares his insights into the role of DPI in lawful intercept, with a focus on the United States.

What is Lawful Intercept?

Lawful intercept or lawful interception of data is the legal term used when an investigative agency seeks court permission to intercept suspect data, cell information and/or location information. This includes the decryption of the data captured and may bring the need to expand monitoring in other countries that will assist under the terms of our mutual treaties for data protection, such as EU Directive 2016/680 of the European Parliament. This directive provides for the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

In the U.S., the Fourth Amendment protects citizens against unreasonable searches and seizures, which has led to a series of laws that dictate formal actions that must be taken by authorities before any type of surveillance or data capture may be permitted.

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA updated the Federal Wiretap Act of 1968, which addressed interception of conversations using "hard" telephone lines, but did not apply to interception of computer and other digital and electronic communications.

Several subsequent pieces of legislation, including The USA PATRIOT Act, PUBLIC LAW 107–56—OCT. 26, 2001, clarified and updated the ECPA to keep pace with the evolution of new communications technologies and methods, including easing restrictions on law enforcement when accessing modern technologies like cell phones, pads, and notebook computers, etc. This update also covered the decryption of hidden and encrypted data on storage devices.

Lawful intercept typically takes one of five forms. The following outlines the most common cases.

When the Federal Government Seeks Data

In the U.S., Intelligence and Federal Law Enforcement agencies, such as the FBI, CIA, NSA, NRO, are allowed to seek a lawful and specific warrant giving them the right to monitor, capture, decrypt certain data streams, but only after a federal judge has evaluated the basis for the warrant and agrees with the content and limits of the warrant's requests. The judge may alter any parts of the warrant before it is granted. The laws regarding this type of data capture were included in the anti-terrorism focused Patriot Act. This also includes the right for the intelligence agencies to decrypt the captured data. The warrant includes the length of time that the captured data may be kept and investigated. Multiple warrants may be issued for many events and data streams to be captured and investigated for use in arresting and charging under the laws of the U.S.

When State and Local Law Enforcement Seeks Data

When local and state Law Enforcement agencies investigate criminal events, i.e., child protection, pornography, abduction (ICAC for Internet Crimes against Children}, murder, kidnapping, etc., a warrant is required for a lawful intercept. Like the federal warrant, local and state warrants must be very specific about the data to be captured and the nature of the criminal activity that is being investigated, as well as the length of time required for the investigation. A judge must sign the warrant and also may change any part of the request to preserve the legality of the investigation.

When Internet Service Providers are asked to Provide Data

Lawful intercept also applies to requests to internet service providers (ISPs) for data related to an investigation. These are limited to alerting law enforcement to suspicious traffic. Suspicious traffic reports are routed to NCMEC (The National Center for Missing and Exploited Children) who pass that data on to the appropriate state or federal agency for lawful investigation. The receiving law enforcement agency must apply for warrants before data can be captured and used in any investigation, arrest and/or prosecution. This is especially important for child protection, where unlawful acts are usually routed to state agencies, and once the location of the offender is determined, local agencies work with the state and possibly federal agencies for warrants for acquisition of evidence, investigation (including decryption), arrests and prosecution.

Companies, such as Google and cell carriers, help with locating children in danger, in distress, kidnapped, assaulted, murdered or victimized within the legal processes required by law.

The Communications Assistance for Law Enforcement Act (CALEA) is a statute enacted by Congress in 1994 that requires telecommunications carriers and manufacturers of telecommunications equipment to design their equipment (cell phones, radios and all communication gear and software), facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information, like location and tracking. CALEA is intended to preserve the ability of law enforcement agencies to conduct controlled electronic surveillance, while protecting the privacy of information outside the scope of the investigation and warrant. In 2005, the Commission extended coverage of CALEA to include all facilities-based broadband Internet access providers and providers of interconnected Voice over Internet Protocol (VoIP) service. CALEA is designed to help locate victims, their positional history, emails, TXT and any applications that may help in a lawful Investigation. They also are instrumental in helping locate lost or abducted children.

When Corporations Monitor their Own Data

Lawful Intercept also applies to corporations that require monitoring of their data for protection of corporate information and to prevent data breaches and illegal access. Many corporations require employees to sign an agreement allowing the company to monitor all traffic through their network and the usage of corporate devices and applications. This capability of data surveillance may be used in employee liability and criminal issues relating to the protection and/or dissemination of corporation data through theft, sale and illegal distribution of corporate secrets, as well assisting in any breach or hack of the network. Corporations may also be able to monitor employees work at home.

When Parents Who Want to Monitor and Protect Their Children

In the case of parents who are looking to monitor and protect their children, lawful intercept concepts apply as well. If a private person wants to oversee what their children are doing on the internet, they can monitor as well as block access to certain sites (COPPA Act aimed at children under 13). This applies to cell phone usage and IoT devices like smart toys. Many states set a maximum age of 13 years old for such monitoring and controls, while other states say as long as a family member is using the parent's internet access, the parents have the right to monitor and control their children's access since they are the responsible party. Almost every state has different laws about this subject. Suggested reading - https://www.google.com/search?q=Cybersecurity+Law+USA+2023

With widespread and growing access to Wi-Fi, we recently have seen community and private Wi-Fi sharing of internet access, sometimes called "subletting access," in which

the users are sometimes called “pawns.” The act of “piggybacking” access may violate many state laws, even with the owner’s permission. The individual responsible for the internet access that is sharing their access through a Wi-Fi connection, or any connection, may be held responsible for the usage by their users. If criminal usage is ascertained, the “owner” of the connection may be culpable in the eyes of the law and will be included in any investigation. Plus, it is generally the policy of ISP’s that one cannot share access, especially for monetary gain. The laws on piggybacking with and without permission are not firm and vary state by state in the U.S.

One last note – Authorities at borders and in international transport areas do have the right to search passenger’s digital media. They may look for criminal events, like drug trafficking and border crossing crimes like illegal entry. The general rule is “reasonable suspicion” and it should be articulated, but does not require authorities to obtain a warrant.

DPI – The Good, The Bad, and The Ugly

Many people blame technologies like DPI for monitoring and controlling sanctioned data. DPI was designed, however, to alert legal corporate users to bad and/or dangerous traffic, and to aid in blocking that dangerous traffic. DPI was created for benevolent purposes, such as detecting and intercepting viruses, worms, spyware, and other forms of malicious data traffic, including intrusion, control (like IoT) and/or takeover attempts. DPI examines the contents of packets passing through a given checkpoint and makes real-time decisions depending packet contents and based on rules assigned by an enterprise, an internet service provider, or a network manager. DPI devices are mostly used in conjunction with a firewall to further protect the network.

Like any device that was designed for good, DPI can be used for illegal eavesdropping and state sponsored censorship. However, DPI devices are expensive and difficult to program by just anyone.

As many as 30 countries worldwide contend that they are committed to protecting their citizen’s data, and many do. Some countries conduct unscrupulous activities against their citizens for political purposes, including spying, and to control the availability of information on the internet. Some 30 countries claim that they have data protection laws. Only a few, however, respect those “laws” and protect their citizen’s information.

Fortunately, U.S. citizens are safeguarded by the strictest data protection laws. Lawful Intercept ensures that the gathering of DPI is done in conformance with the law.