# Global Information Assurance Certification Paper

# Next-Generation Firewalls and Employee Privacy in the Global Enterprise

*GIAC (GLEG) Gold Certification*

Author: Ryan Firth, RyanQFirth+gleg@gmail.com
Advisor: Rob VandenBrink

Accepted: September 21st 2014

Abstract

By year-end 2014, Gartner predicts that 70% of new firewall purchases will be next-generation firewalls. (Young, 2013) Organizations are quickly realizing the practical benefits of combining deep packet inspection, application awareness, IPS/threat detection, VPN, SSL interception, web filtering, and traditional firewall functionality into a single platform.

With the ease of deploying such a powerful toolset in a single perimeter device, considering the international laws of employee privacy can become an afterthought.

Can an organization protect themselves by simply providing notice to employees in any country that their Internet activity is being monitored? Does SSL interception create a greater liability to the company? Does monitoring employee Internet traffic actually create greater risk?

This paper will explore these and other legal issues surrounding network monitoring and employee privacy in the U.S., European Union, and other selected countries in other parts of the world.

# 1. Introduction

## 1.1. Network monitoring and employee privacy

An obligation to protect company resources is something nearly every organization tries to instill in their staff. Through advances in technology, new ways of protecting network resources are continuously released—some requiring serious legal consideration. IT and legal departments are wise to pay close attention to any technology that could allow intrusion into the actions of employees. Although employers in the United States are allowed a high level of freedom to override employee privacy in the name of protecting company assets, other countries may provide the employee with far greater privacy rights.

Recent revelations over U.S. mass spying efforts have added fuel to the contentious debate over Internet privacy. While the issue of Internet privacy for a citizen is a much different conversation than that of an employee, the underlying concerns will undoubtedly carry over into the workplace.

Employers with highly restrictive Internet and monitoring policies may stifle new and innovative uses of Internet technology, or otherwise unknowingly harm employee productivity. One survey of 745 employees over eight operating companies indicated that, "… employees who had their performance electronically monitored perceived their working conditions as more stressful, and reported higher levels of job boredom, psychological tension, anxiety, depression, anger, health complaints and fatigue." (Smith et al., 1992) Although Smith's research was carried out in a much different era of technology, analogous conclusions were seen by O'Donnell et al., (2013) who demonstrated that "…surveillance, where it is not needed, can do more harm than good." Additional negative conclusions were discovered through employee surveys by Coultrop & Foutain (2012), as well.

On the other side of the employee privacy argument, an organization choosing not to monitor or restrict Internet activity in any way may open itself up to legal risks such as

sexual harassment lawsuits[1], copyright violations[2], or child pornography litigation[3]. Additionally, without proper Internet monitoring controls in place, performing network forensics such as in the case of a data breach, may not be possible. Analyzing network traffic can sometimes be the only way to detect compromised computers on the corporate network.

From an information security and legal perspective, an organization is wise to monitor their company's Internet traffic in accordance with the law. Technology exists to provide complete surveillance; the question is how to perform this function ethically and legally across global legal boundaries where the issue of employee privacy may differ significantly from one country to the next.

## 1.2. Traditional and next-generation firewalls

In 1994, Check Point Software released the first commercial stateful firewall to market.[4] Stateful firewalls are usually considered "traditional" firewalls, and focus primarily on two pieces of information—IP addresses and port numbers. Depending on what other capabilities a manufacturer bolts on to these traditional firewalls, it may be possible to gather additional information, but this is highly specific to the firewall in use.

Next-generation firewalls (NGFWs) started gaining attention around 2009. Gartner released a brief paper that year on the subject titled, "Defining the Next Generation Firewall".[5] There was a growing realization of the benefits of more advanced features such as, "integrated deep packet inspection, intrusion detection, application identification, and granular control"(Young, 2009) which spurred the growth of the NGFW market.

Firewalls are transitioning from providing basic numbers—in the form of IP addresses and ports—to the ability to recreate and analyze an employee's complete online

[1] http://madisonrecord.com/news/201856-madison-county-secretary-files-sexual-harassment-suit-against-county
[2] https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/359/vol1_no2_art7.pdf?sequence=1 (p. 1)
[3] http://www.metrocorpcounsel.com/articles/6569/when-employee-surfs-internet-kiddie-porn-work-avoiding-civil-liability-employee-cyber-
[4] http://www.checkpoint.com/press/1994/interop_press.html
[5] http://blogs.gartner.com/greg_young/2009/10/15/defining-the-next-generation-firewall-research-note-the-liner-notes/

experience. In a global enterprise, the IT and legal teams may have developed an employee privacy policy with traditional firewall functionality used as the basis of their strategy. A legal team may have no idea that a firewall could continuously collect sensitive personal details of Internet activity such as Google search terms, account information, web browsing history, phone conversations, credit card numbers, or protected health information.

## 1.3. Research Scope

NGFW manufacturers have similar feature sets, although a particular manufacturer may advance a specific function in an effort to set them apart from their competitors. This paper will focus on the capabilities of Palo Alto Networks' next-generation firewalls, a consistent leader in Gartner's "Magic Quadrant for Enterprise Network Firewalls" report.[6] Specific features such as web filtering, traffic logs leveraging deep packet inspection, and SSL interception will be explored. It is impractical to analyze employee privacy laws in every country, so a few sample countries and regions will be used to frame the discussion, including: The United States, the European Union, the Philippines, and India.

Specific laws or case rulings regarding employee privacy and NGFWs are unlikely to exist. Instead, the goal of this paper is to understand the basic principles of employee privacy in each sample country, then extrapolate the application of those principles to the capabilities provided in NGFWs.

Perhaps most importantly, this paper will discuss how to locate reliable information on international employee privacy. These methods can assist in creating an informed legal policy in other areas of employee privacy such as video surveillance, email privacy, keyloggers, phone monitoring, etc. A global enterprise will most likely require privacy policies to address these other areas of employee monitoring. Policies on network monitoring derived from recommendations in this research paper would then plug in to the larger corporate framework on employee privacy. While it is possible to intercept email messages and IP phone conversations through a firewall's packet sniffer, an organization should view the routine collection and analysis of either as a different

[6] http://www.gartner.com/technology/reprints.do?id=1-1T607HL&ct=140415&st=sb

legal issue than one of network monitoring. The U.S. ECPA (Electronic Communications Privacy Act) specifically addresses the intentional intercept and monitoring of email and phone conversations.

This paper is not a substitute for legal advice or legal counsel. Information security law can change quickly; therefore, an organization should not rely on this body of research alone to determine employee privacy or monitoring policy.

# 2. Monitoring capabilities of a next-generation firewall

## 2.1. User attribution and enhanced traffic inspection

A firewall's tighter integration with directory services, such as Microsoft Active Directory, allows organizations to enforce security policy based on user ID or group membership instead of IP address. By extension, this can automatically tie the user's ID to the firewall's logs and other traffic reports. It should be noted that this is not an exclusive feature of NGFWs, as traditional firewalls may also allow directory integration; however, combined with the rich new features of NGFWs, compiling a detailed report on an employee's Internet behavior can reveal far more than ever before.

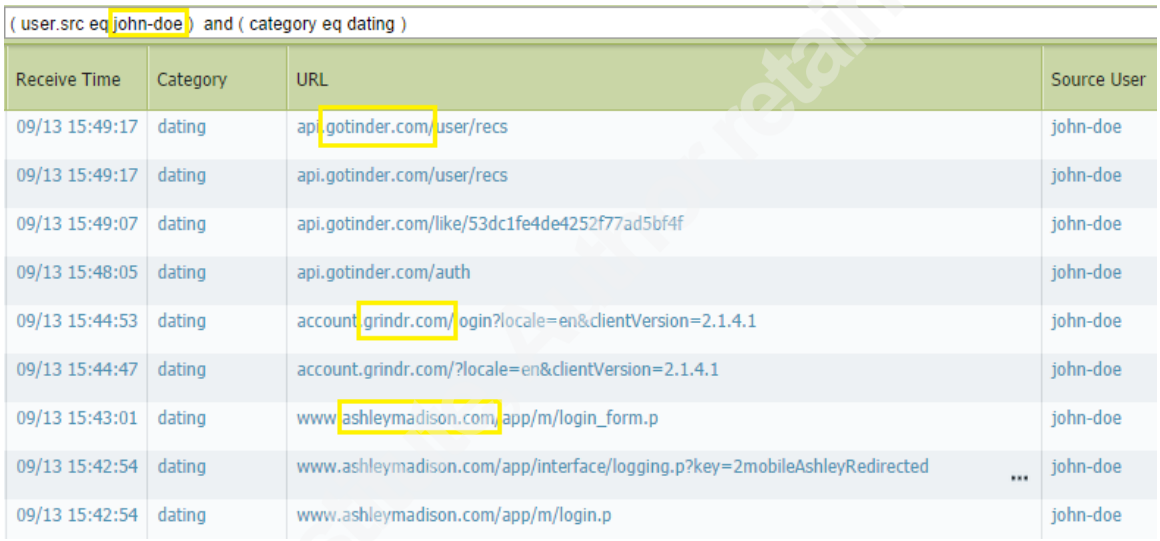
In Figure 1, the employee John Doe is found using Google, Bing, and Yahoo to search for the personal and sensitive terms, "find an oncologist", "cancer treatments", "cost of filing bankruptcy", "divorce attorneys", "how to tell your kids you're pregnant", "aids treatments", and "keep from transmitting aids to partner".

( user.src eq john-doe ) and ( url contains '/search')

| Receive Time | Category | URL | Source User |
|---|---|---|---|
| 09/13 15:20:45 | search-engines | search.yahoo.com/search;_ylt=AuO1meLgSK_DzFFz2xeAG.KbvZx4?p=find+an+oncologist&... | john-doe |
| 09/13 15:20:10 | search-engines | search.yahoo.com/search;_ylt=A0LEVw6cphRU8GkA7tNXNyoA;_ylc=X1MDMjc2NjY3OQRfcg... | john-doe |
| 09/13 15:18:36 | search-engines | search.yahoo.com/search;_ylt=A2KLtYF4phRU1BAAE4ibvZx4?p=cancer+treatments&toggle... | john-doe |
| 09/13 15:17:06 | search-engines | www.bing.com/search?q=cost+of+filing+bankruptcy&qs=AS&pq=cost+of+filing+b&sc=8-... | john-doe |
| 09/13 15:16:48 | search-engines | www.bing.com/search?q=divorce+attorneys&go=Submit&qs=n&form=QBLH&pq=divorce+... | john-doe |
| 09/13 15:16:33 | search-engines | www.google.com/search?q=how+to+tell+your+kids+you're+pregnant&oq=how+to+tell+y... | john-doe |
| 09/13 15:16:08 | search-engines | www.google.com/search?q=aids+treatments&oq=aids+treatments&aqs=chrome..69i57.31... | john-doe |
| 09/13 15:15:56 | search-engines | www.google.com/search?q=keep+from+transmitting+aids+to+partner&oq=keep+from+&... | john-doe |

Figure 1. Web search engine queries made by the employee John Doe

Figures 2 and 3 provide an example of the employee's phone connecting to Tinder, (What GQ describes as a "dating-hookup" app)[7] Grindr, (An app to "Find local gay, bi and curious guys")[8], and Ashley Madison, whose tagline is "Life is short. Have an affair."[9] This employee's phone could simply run these applications in the background, without the user actually interacting with any of them while at work. For a straight, married, high-ranking executive of a prestigious company, this type of information could be incredibly damaging.



( user.src eq john-doe ) and ( category eq dating )

| Receive Time | Category | URL | Source User |
|---|---|---|---|
| 09/13 15:49:17 | dating | api.gotinder.com/user/recs | john-doe |
| 09/13 15:49:17 | dating | api.gotinder.com/user/recs | john-doe |
| 09/13 15:49:07 | dating | api.gotinder.com/like/53dc1fe4de4252f77ad5bf4f | john-doe |
| 09/13 15:48:05 | dating | api.gotinder.com/auth | john-doe |
| 09/13 15:44:53 | dating | account.grindr.com/login?locale=en&clientVersion=2.1.4.1 | john-doe |
| 09/13 15:44:47 | dating | account.grindr.com/?locale=en&clientVersion=2.1.4.1 | john-doe |
| 09/13 15:43:01 | dating | www.ashleymadison.com/app/m/login_form.p | john-doe |
| 09/13 15:42:54 | dating | www.ashleymadison.com/app/interface/logging.p?key=2mobileAshleyRedirected | john-doe |
| 09/13 15:42:54 | dating | www.ashleymadison.com/app/m/login.p | john-doe |

Figure 2. The employee's phone is accessing gay, hookup, and affair sites.

Figure 3 is an example of the Tinder application identified by its signature, instead of by IP, URL, or port. In other words, the ability for applications to hide from an NGFW is very difficult by design. As applications integrate even further into everyday life, and the boundaries continue to blur between personal and work activity online, the concern around privacy in the workplace will continue to grow.

[7] http://www.gq.com/life/relationships/201402/tinder-online-dating-sex-app
[8] http://grindr.com/
[9] https://www.ashleymadison.com/

Ryan Firth, RyanQFirth+gleg@gmail.com

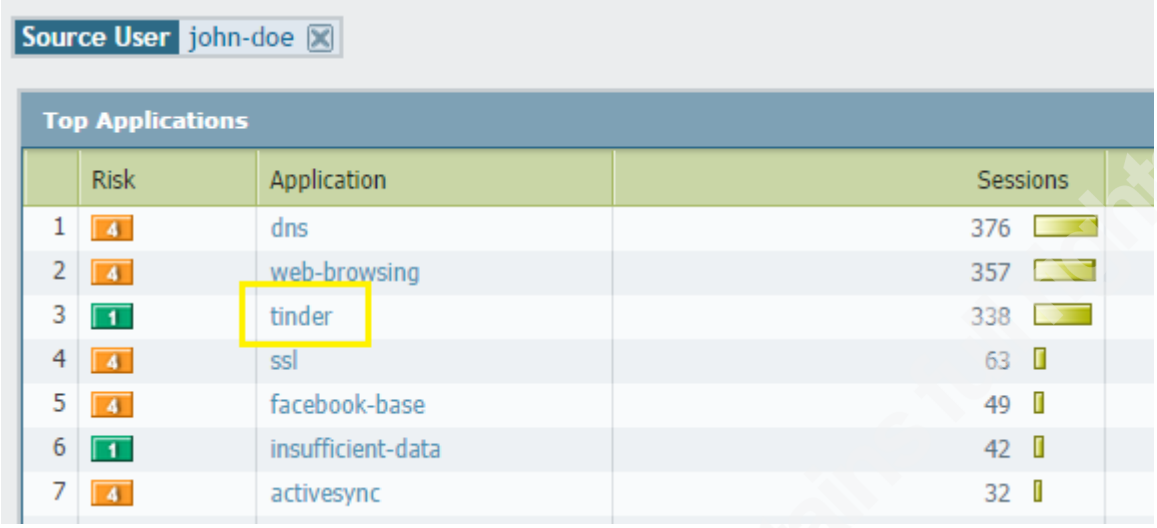



Figure 3. The "Tinder" application is identified by application signature for the employee John Doe.

## 2.2 SSL interception

Figure 1 above displays Google search terms typed by the employee. In late 2013, however, Google started to encrypt all keyword searches.[10] If Google search is encrypted, how is the firewall able to see the employee's search query? The answer is SSL interception, also known as an SSL forward proxy or simply SSL decryption. Acting as a "man-in-the-middle", the firewall negotiates an SSL session with the destination server, then separately with the source computer. If an organization's private Certificate Authority certificate is properly installed on a workstation, the user's browser will never display a warning about the SSL interception. Figure 4 provides a general overview of SSL interception in a Palo Alto firewall.

[10] http://searchengineland.com/post-prism-google-secure-searches-172487

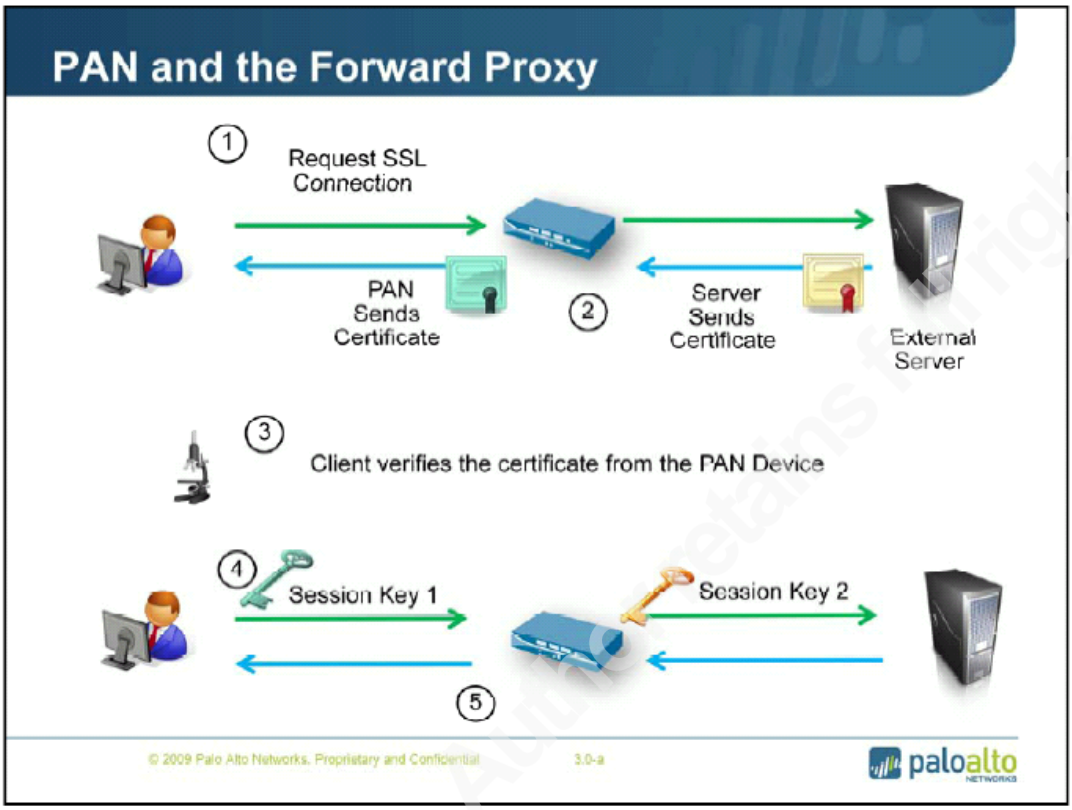



Figure 4. SSL interception/SSL forward proxy (swhyte, 2010)

While users may feel this is an excessive invasion of privacy, SSL interception is becoming essential to detect malicious network traffic. In 2013, the "Gameover" variant of the Zeus Trojan family, one of the largest botnets in history, began encrypting its communication traffic.[11] When workstations are infected with malware, host defenses such as antivirus, host IPS, or the host's firewall have failed in preventing infection. Detecting malicious network traffic from infected workstations is one of the only scalable ways to combat this risk.

Fortunately, SSL interception is usually not an all-or-nothing function. Figure 5 shows a decryption policy where only certain potentially malicious URL categories are decrypted. Under this example policy, the firewall will not decrypt websites in the banking/financial, dating, healthcare, search engine, and other categories. The encrypted Google search terms in figure 1 would not be visible with this policy in effect. As will be

[11] http://www.scmagazine.com/gameover-trojan-hides-activity-in-encrypted-ssl-connections-to-defraud-victims/article/315215/

discussed later in this paper, employer restraint and monitoring only what is necessary for protecting the business is heavily favored in the courts of many countries, especially those in the European Union.

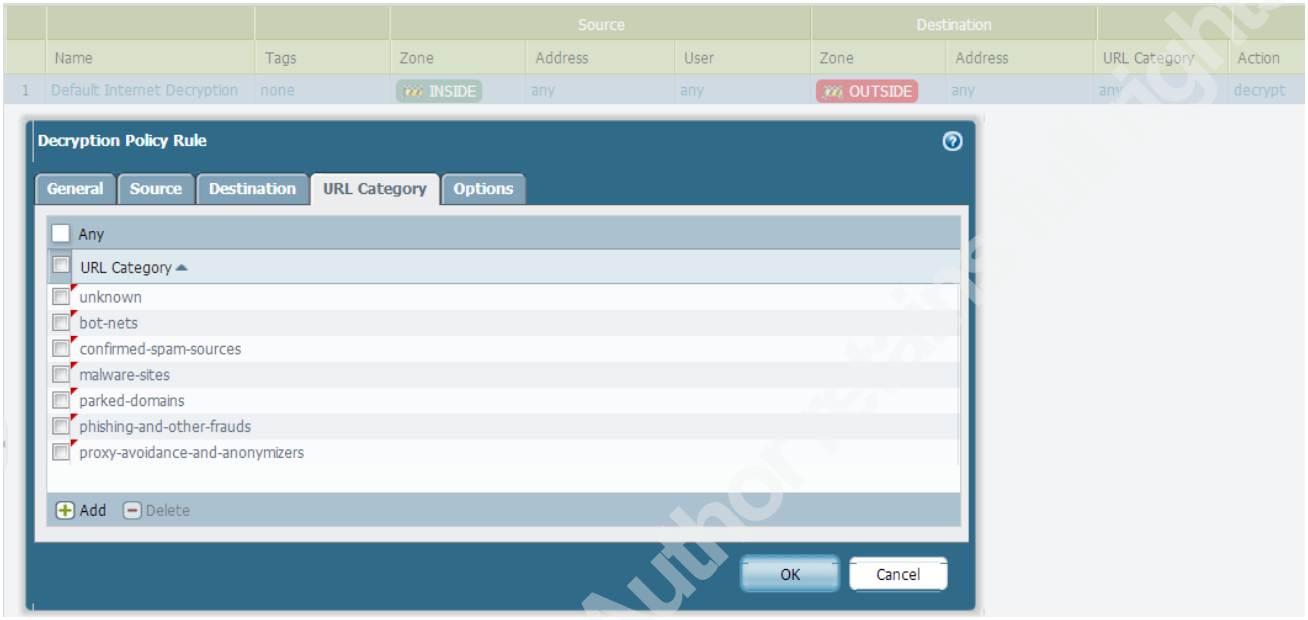



Figure 5. A Palo Alto decryption policy focused only on potentially malicious URL categories.

It is assumed throughout this paper that, where legally feasible, an organization wishes to utilize the full capabilities of NGFWs to help secure their environment. Collecting and processing the sensitive personal data shown in the above section creates an obligation for the organization to adhere to strict requirements in certain countries, which will be explored below.

## 3. Obtaining reliable legal information and opinions

Organizations should ultimately lean on legal counsel to provide reliable guidance on employee privacy policies, domestic and abroad. In-house counsel, however, cannot be expected to have up-to-date expertise on every privacy law in every province and country throughout the world. Outside counsel—typically large international law firms—can leverage attorneys with specific expertise in the country of interest. Legal referral services help organizations choose an appropriate law firm if in-house counsel is not available. Moving forward with an employee monitoring program without legal advice is certainly an option, though there is an inherit risk to this strategy if the

organization is ever called in front of a court. The ethics of potentially violating the privacy rights of individuals in their country should hopefully be of moral concern, as well.

Privacy laws are usually handled by a country's Data Protection Authority (DPA) or office of similar title. A DPA's website will provide privacy guidance in varying levels of usefulness, depending on the country involved. Examples of excellent DPA websites include Canada (https://www.priv.gc.ca/), Ireland (https://www.dataprotection.ie), and France (http://www.cnil.fr/english/). These sites provide excellent documentation, educational material, and other guidance to help citizens and business understand privacy rights in their country. An official DPA does not exist in the U.S., however, the FTC and state attorneys general assume similar responsibilities.

Contacting a DPA through email for clarification on privacy law may yield some benefit. Ten countries across multiple continents were emailed specific questions around employee privacy in their respective country throughout the course of this writing. Four DPAs, three of whom reside in the E.U., responded with actual, non-canned, guidance.

Privacy law desk references, or their electronic counterparts, can be great sources of information. *Global Employee Privacy and Data Security Law, Second Edition*, published in 2011, provides 770 pages of legal analysis on privacy laws around the world. Electronic references, which can provide up-to-date information more quickly than printed text, include:

- Baker & McKenzie's Global Privacy Handbook
- DLA Piper – Data Protection Laws of the World
- Norton Rose Fulbright – Global data privacy directory
- Linklaters – Data Protected
- Mayer-Brown – Employee Data Privacy–A Global Overview

Ryan Firth, RyanQFirth+gleg@gmail.com

- Morrison Foerster – Privacy Library (Online)[12]

Legal blogs and other online articles and postings are useful for up-to-date insight on privacy law, where court decisions challenging or strengthening the established interpretation of statues are dissected and discussed. It is best to find reputable websites and blogs in the country where privacy policies are to be created. Examples include: Benjamin Wright's Google+ blog,[13] The Canadian Privacy Law Blog,[14] and the Fieldfisher Privacy and Information Law Blog,[15] for a UK and European focus.

## 4. Global employee privacy law

It is no surprise that privacy laws vary significantly throughout the world—from non-existent, as is the case with many African countries, to the exhaustive policies established by many countries in the European Union. DLA Piper, a global law firm, illustrates this point in the heat map below.

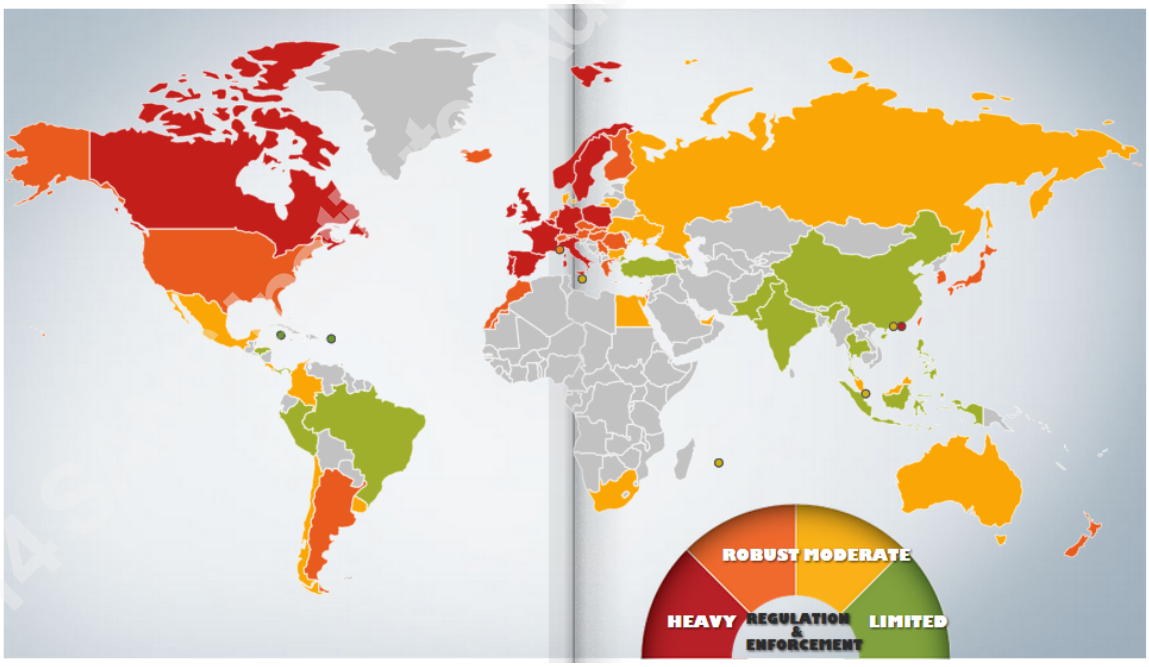



Figure 6. A heat map of privacy regulations and enforcement throughout the world. (DLA Piper, 2014)

[12] http://www.mofo.com/privacylibrary/PrivacyLibraryLanding.aspx?xpST=PrivacyLibraryLanding
[13] https://plus.google.com/u/0/+BenjaminWright1/posts
[14] http://blog.privacylawyer.ca/
[15] http://privacylawblog.fieldfisher.com/

Ryan Firth, RyanQFirth+gleg@gmail.com

First, a few sample countries and regions will be explored as an introduction to employee privacy laws, or lack thereof. Common requirements and themes will then be explored, along with recommendations for crafting a global enterprise privacy policy.

## 4.1. The United States

In terms of network surveillance and monitoring, privacy law in the U.S. is generally derived from the ECPA (Electronic Communications Privacy Act of 1986).[16] As stated from the U.S. Department of Justice website, "The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers." (2013). Employers, however, are largely exempt through one of two statutory exceptions. Section 18 U.S.C. Part I, chapter 119, § 2511, (2), (a), (i) states:

> It shall not be unlawful . . . for . . . a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks. (Harvard Law School, n.d.)

The second exemption is that of consent, whereby an employer need only inform employees under surveillance. While it is common practice to inform employees, the first statutory exemption makes this largely unnecessary.

Unfortunately, with the brief exceptions above, laws specifically addressing employee privacy do not exist at the federal level. Of all state laws regarding this issue, only Connecticut and Delaware require employers to give notice to employees before monitoring their Internet traffic. The National Conference of State Legislatures maintains a webpage dedicated to "State Laws Related to Internet Privacy" with a section

[16] http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

dedicated to "Notice of Monitoring of Employee E-mail Communications and Internet Access" (2014).

In addition, an organization's Internet monitoring capabilities and requirements may change if either public or union employees are involved. Public employees may enjoy additional limited rights through the U.S. Constitution, while the National Labor Relations Act (NLRA) and collective bargaining agreements could provide surveillance restrictions around union employers.[17]

## 4.2. European Union

The European Union's overarching privacy policies are currently guided by the Data Protection Directive (DPD). Adopted in 1995, this non-binding policy provided guidance for each member country as they enacted their own privacy legislation. For a global enterprise operating throughout Europe, it's important to understand that each country enacts their own privacy laws. As a result, the DPD cannot be used as the ultimate legal foundation for employee privacy policies.

Conforming to each European country's specific privacy laws can be difficult if an enterprise exists in several countries across the E.U. In an effort to address these concerns, and address new privacy issues not currently covered by the DPD, the European Commission is spearheading the General Data Protection Regulation (GDPR). If adopted, this is expected establish a unified privacy law throughout the European Union. While a unified law is much easier to adhere to, proposed fines for violation of the GDPR is expected to be substantial—100,000,000 Euros or 5% of global turnover.[18] Adoption of the GDPR is expected in late 2014 or early 2015, with the regulation taking effect two years after adoption.[19]

The Data Protection Working Party, Article 29, offers a Working Document (WP55) providing employer guidance "on the surveillance of electronic communications in the workplace." (Data Protection Working Party, 2002) WP55 provides guidance and insight to help corporate policymakers understand European employee privacy principles.

[17] https://www.privacyrights.org/ar/employees-rights.htm
[18] http://www.europarl.europa.eu/news/en/news-room/content/20140307ipr38204/html/MEPs-tighten-up-rules-to-protect-personal-data-in-the-digital-era
[19] http://ec.europa.eu/justice/data-protection/

The issue of employee consent in the E.U. is particularly interesting when crafting employee privacy strategy. The "Opinion 15/2011 on the definition of consent" by the Article 29 Data Protection Working Party of the E.U. states:

> Where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent.… An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut where, as is often the case, all employers impose the same or a similar condition of employment. (Article 29 Data Protection Working Party, 2011)

Stated another way, an employee's consent is invalid if he is not able to opt out without consequence. This proves to be a challenge when an enterprise attempts to secure its infrastructure by monitoring Internet traffic. Permitting all traffic without inspection from any employee who chooses to opt out is untenable and poses high risk.

The balance of an organization's right to secure their assets while respecting an employee's right to privacy is an acknowledged difficulty. The key to this balance lies in a concept pervasive in data protection laws throughout the E.U.—proportionality. That is, there must be adequate justification for the degree of privacy lost by the employee. In an extreme example, it would not be proportionate to install keyloggers[20] on all employee computers for the purpose of tracking employee productivity. A balance must be struck. An organization displaying restraint in their monitoring practices, and solid justification for the techniques used, is seen in a more favorable light when issues of employee privacy are brought to E.U. courts.

[20] Software or hardware used to capture all keystrokes entered in a computer.

## 4.3. Philippines

Although there are no laws specifically addressing an employer's ability to intercept and monitor an employee's Internet usage in the Philippines, general privacy rules apply. These laws are defined in the Data Privacy Act of 2012, also known as Republic Act 10173.[21] Provisions in the Cybercrime Prevention Act of 2012, also known as Republic Act 10175, the Philippine Constitution, the Civil Code of the Philippines, and the Anti-Wiretapping Law may also provide legal insight. Existing privacy laws do not specifically define employee privacy rights; employees are simply treated as any other individual in this regard.

Employee Internet usage could divulge information falling into two classifications of data defined by the Data Privacy Act of 2012—"Personal Information" and "Sensitive Personal Information". The most applicable way for an employer to legally collect this information is in the form of consent. According to the Act on the legal processing of sensitive personal information and consent, "The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing" (Republic of the Philippines, 2012) Unlike some countries in the E.U., employee consent in the Philippines is considered a valid way to waive certain privacy rights.

What if an employee does not consent? According to the Bureau of Labor Relations[22], this would not constitute grounds for terminating the employee. In certain situations, "retrenchment to prevent losses" may provide legal justification for termination upon refusal of consent. Whether or not the potential future losses suffered as a result of a security breach due to a lack of Internet monitoring could be considered substantial and imminent—a requirement for this rationale of termination[23]—would need to be established through court rulings.

A policy whereby all personal Internet access is only permitted from employees' personal devices over a minimally-monitored and completely separate "guest" Internet circuit may provide an alternative to gaining employee consent for monitoring the

[21] http://www.gov.ph/2012/08/15/republic-act-no-10173/
[22] http://blr.dole.gov.ph/index.php/faqs/termination-of-employment
[23] http://sc.judiciary.gov.ph/jurisprudence/2009/september2009/181503.htm

Ryan Firth, RyanQFirth+gleg@gmail.com

organization's main Internet circuits. This strategy will be explored in further detail later in the paper.

Although an appointment of a data protection officer is not specifically required by the Data Privacy Act of 2012, an organization is required to "… designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request." (Republic of the Philippines, 2012) For proper separation of duties, and to avoid conflicts of interest, these individuals should exist in the compliance or legal departments of an organization.

## 4.4. India

India's employee privacy laws, like other developing countries, are only recently starting to emerge. In April of 2011, the Ministry of Communications and Information Technology released a notification titled, "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011."[24] Clarifications to these rules were issued as a "press note" on August 24th, 2011.[25] The Information Technology (Amendment) Act of 2008 includes protections of sensitive personal information.[26] As expected, case law related to employee Internet privacy under these regulations has not been well established as of this writing.

Obtaining informed employee consent, along with following other legal requirements set forth in the above laws, should allow for lawful monitoring of employee Internet access. There is an obligation for the employer to provide a privacy policy viewable by any employee in which sensitive personal information may be collected. As with privacy law in many other countries, the right for an employee to opt out must exist. Labor laws again dictate the employer's acceptable response to an employee opt-out. In addition, an organization processing sensitive data must appoint a Grievance Officer for correction requests, complaints, and employee access to their collected data.

[24] http://deity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf
[25] http://www.gibsondunn.com/publications/pages/GovernmentofIndia-ClarificationstoDataPrivacyRules.aspx
[26] http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

## 4.5. Common themes and requirements

Established policies

Outlining what is, and is not, an appropriate use of technology is highly recommended, and in many countries a requirement, before collecting sensitive personal data. An acceptable use policy (AUP) is the most appropriate method for disseminating these policies.

Enterprises are often required to establish privacy policies detailing: 1) What data will be collected 2) How the data will be used 3) Why the collection of sensitive information is necessary 4) How long the data will be kept, and 5) Who in the organization an employee can request access to their collected personal data, or to file a privacy grievance.

Establishing a security policy describing how sensitive personal data is to be secured is also a common requirement. Verifiable consent by the employee is important for both the AUP and privacy policies.

Registration with a data protection agency

It is common throughout the E.U. and many other countries with strict laws on data privacy to require organizations who collect, process, or store sensitive personal data to register with the country's data protection agency. Sometimes only certain industries, such as the financial sector, falls into this requirement.

Appointment of a data protection officer

A data protection officer, or position of similar function, is often either required or recommended. This requirement may come into effect only for organizations over a certain size, or within a particular industry. The data protection officer is usually responsible for ensuring that the organization is adhering to data privacy laws of the given country. Employees should also be able to reach out to the data protection officer for access to their collected personal data, or to file a privacy grievance.

Establish transfer requirements

If sensitive personal data is to be transported out of certain countries or regions, as would be the case if a NGFW in Europe sends logs to a central log collector located in the U.S., special rules may apply.



Ryan Firth, RyanQFirth+gleg@gmail.com

# 5. Action steps

## 5.1. Creating global privacy policies

Ultimately, an organization with international presence is forced to utilize one of three approaches to employee privacy—"lowest common denominator", "individualized", or a "categorical" approach.

Under a "lowest common denominator" approach, an organization adopts a single global privacy policy that adheres to the most stringent privacy requirements. This policy should not only encompass privacy strategy encompassing all countries with existing offices, but countries the organization has a decent chance of operating in sometime in the future as well. Although this may unnecessarily create administrative burdens in countries of low privacy requirements, having a single policy to create, review, and update worldwide may be less of a burden overall.

In an "individualized" approach, a separate privacy policy is created for each country. This strategy may be most appropriate for enterprises operating in only a few countries that all have significant differences in privacy laws. A "categorical" approach is a hybrid of the two prior strategies. By grouping countries of similar privacy requirements, such as all countries residing in the E.U., fewer policies are maintained, while not creating unnecessary overhead in those countries where privacy policies are lax.

The following are general action steps to establish a "lowest common denominator" privacy policy for a global enterprise wanting to deploy and fully utilize NGFWs, or Internet monitoring devices of similar functionality:

- Determine where Internet monitoring fits into the larger employee privacy framework of the organization. Is corporate email monitored? Are video cameras monitoring employee activity? Are employee phone calls monitored, as is common in a call center? Is surveillance software installed on computers? Privacy writers must address, or at least consider, the legal obligation for these areas.

- Establish which countries' privacy policies should come into play. Countries where a presence already exists should obviously be included, but to establish and maintain a solid global policy, future locations should be considered. Top executives, especially those responsible for mergers and acquisitions, can provide this insight.
- Determine if the organization employees individuals requiring special privacy rights. Union workers or public employees are the most common individuals in this area.
- Determine where the data will reside. If sensitive personal data moves outside of the country or region where the data was collected, special obligations could apply.
- Appoint a data privacy officer. Many countries require or recommend that enterprises establish this appointment, but it is best practice to do so even without legal obligation. This position is responsible for ensuring a company adheres to all relevant privacy policies, and should exist in the legal or compliance areas of an organization. By virtue of this position residing outside of I.T., proper separation of duties is established. Employee grievances concerning data privacy as well as requests for the employee's collected personal information are handled through this position.
- Establish an acceptable use policy (AUP) to inform employees what is, and is not, an acceptable use of technology. This policy should be presented and acknowledged upon employment and re-acknowledged at least annually. The AUP should be acknowledged by non-employees using corporate services, as well, such as in the case of guest Internet access.
- Establish a privacy policy detailing:
    a. What data will be collected
    b. How the data will be used
    c. Why the collection of this data is necessary
    d. How long the data will be kept

e. Who in the organization an employee can request access to their collected personal data, or file a privacy grievance

Certain countries may require an organization to provide employees with an opt-out for the collection of sensitive personal data. If this is a requirement, establishing how systems will accommodate the opt-out is necessary.

- Determine which countries require registration with a data protection authority or similar office.
- Create a comprehensive document detailing breach notification laws of each country. If sensitive personal data is compromised, many breach notification laws require quick action to stay in compliance.
- Establish a schedule for appropriate parties to periodically review relevant privacy laws, and to update the items listed above.

## 5.2. An alternate approach

In cases where an enterprise does not have to contend with employee privacy issues in other areas of the workplace, an alternate approach can be considered for deploying NGFWs or devices with similar Internet monitoring functionality. This approach may also be appropriate where an enterprise's IT department is ready to deploy NGFWs globally, but the organization's privacy framework is still months or years away from proper completion.

Concerns surrounding employ monitoring center around the collection of sensitive personal information mixing in with business traffic. A publication produced by data protection authorities in Poland, Czech Republic, Croatia, and the Republic of Bulgaria poses the question, "Is the monitoring of my work e-mails and Internet access on behalf of the employer processing of personal data?" to which it answers "…It is hard to distinguish clearly which activities form part of your professional or business life and which fall to your private life, too For this reason it is accepted that e-mail and Internet access monitoring in the workplace is indeed personal data processing." (Lifelong Learning Programme, 2012)

But what if it was not hard to distinguish between data from an employee's private and professional life? For purposes of monitoring business Internet traffic, while avoiding the collection of employee Internet traffic, the following action steps are proposed. Court rulings, unfortunately, are the only way solutions such as these can be declared as conforming to the law. Seek the opinion of legal counsel before implementing this strategy in countries where great concern over employee privacy exist.

1. Provision a separate guest Internet circuit completely separate from any Internet circuit where business will be conducted.
2. Purchase a separate firewall for the guest Internet circuit. Some firewalls, such as most Palo Alto models, allow separation into multiple logical firewalls.[27] If separation of policy and data collection is achieved, this is an acceptable option.
3. Establish a guest wireless network with an appropriate AUP click-through for acceptance.
4. For the Internet circuit, configure only security options that would not classify as the collection or processing of sensitive personal data. A review of privacy laws for each relevant country is necessary to remain in compliance.
5. Establish an AUP for these offices prohibiting both personal Internet use on business Internet connections, and business use on the guest wireless network.

With the proliferation of smartphones, tablets, and other mobile devices, requiring employees to use a separate wireless network for personal Internet use should not create a substantial burden to employees. For those without personal mobile devices, computers hooked to the guest Internet circuit could be set up for personal Internet use.

[27] https://live.paloaltonetworks.com/docs/DOC-3892

## 6. Summary

Those only familiar with U.S. employee privacy policies may be surprised at how other countries approach the subject—especially countries in the E.U. While an enterprise in the U.S. is, in most cases, permitted to monitor Internet traffic with impunity and without even notifying their employees, other countries side in favor of the worker and do not allow employees to legally waive their right to personal privacy in the workplace.

Next-generation firewalls provide deep insight into network traffic, exposing almost anything an employee does online—and the technology providing this inspection will only get better. As we integrate our lives with applications connected to the Internet, privacy is becoming an increasingly important topic.

Ryan Firth, RyanQFirth+gleg@gmail.com

## 7. References


Young, G. (2014, February 7). *Magic Quadrant for Enterprise Network Firewalls 2013*. Retrieved August 16, 2014, from http://www.bradreese.com/blog/11-27-2013.pdf

Defining The Next Generation Firewall Research Note: The Liner Notes. (2009, October 15). Retrieved from http://blogs.gartner.com/greg_young/2009/10/15/defining-the-next-generation-firewall-research-note-the-liner-notes/

Young, G., Hils, A., & D'Hoinne, J. (2014, April 15). *Magic Quadrant for Enterprise Network Firewalls*. Retrieved August 15, 2014, from http://www.gartner.com/technology/reprints.do?id=1-1T607HL&ct=140415&st=sb

Smith, M. J., Carayon, P., Sanders, K. J., Lim, S. Y., & Legrande, D. (1992). Employee stress and health complaints in jobs with and without electronic performance monitoring. *Applied Ergonomics*, *23*(1), 17–27.

O'Donnell, A. T., Ryan, M. K., & Jetten, J. (2013). The hidden costs of surveillance for performance and helping behaviour. *Group Processes & Intergroup Relations*, *16*(2), 246–256. doi:10.1177/1368430212453629

*Electronic Communications Privacy Act of 1986*. (2013, July 30). *Privacy & Civil Liberties*. Retrieved August 15, 2014, from https://it.ojp.gov/default.aspx?area=privacy&page=1285



Ryan Firth, RyanQFirth+gleg@gmail.com

Coultrop, S., & Foutain, P. D. (2012). Effects of Electronic Monitoring and Surveillance on the Psychological Contract of Employees: An Exploratory Study. *J. Bus. & Behav. Scis.*, *19*, 219.

*State Laws Related to Internet Privacy*. (2014, January 23). Retrieved August 15, 2014, from http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

Harvard Law School. (n.d.). *PRIVACY IN THE WORKPLACE*. Retrieved August 17, 2014, from http://cyber.law.harvard.edu/privacy/Module3_Intronew.html

swhyte. (2010, March 8). SSL Forward Proxy (Man in the Middle). Retrieved August 30, 2014, from https://live.paloaltonetworks.com/docs/DOC-1327

Republic of the Philippines. (2012, August 15). Republic Act No. 10173. Retrieved August 31, 2014, from http://www.gov.ph/2012/08/15/republic-act-no-10173/

DLA Piper. (2014, January). Global Data Protection Handbook. Retrieved September 14, 2014, from http://www.dlapiperdataprotection.com/#handbook/world-map-section

Lifelong Learning Programme. (2012). Privacy protection in the workplace - Guide for employees. Retrieved from

Ryan Firth, RyanQFirth+gleg@gmail.com

http://www.uoou.cz/en/VismoOnline_ActionScripts/File.ashx?id_org=200156&id_dokumenty=1168



Ryan Firth, RyanQFirth+gleg@gmail.com