Let it Snowden!

Thomas A. Gwosdz
City Attorney
Victoria, Texas
(361) 485-3520
tgwosdz@victoriatx.org

Four of Thomas's five children are teenagers this year, including a soon-to-be 19 year old son, a daughter who turned sixteen last week, and twin thirteen-year-old sons.

Thomas has therefore adopted an official department policy requiring "warm, clean and [most of all] calm" client service. Thomas has represented the City in numerous real estate transactions (including the purchase of property for a proposed wastewater treatment plant), a few successful economic development projects (including the final assembly plant for large yellow-and-black hydraulic excavators), and exactly zero criminal indictments (zero and counting).

Thomas was staff attorney at the Texas Association of School Boards, where he enjoyed both travelling the state teaching school board members why they couldn't fire the football coach, and coming home to a small house in the Texas hill country filled to the brim with five wonderful children and a strong Texas woman.

Thomas has also represented large corporate clients in transactions involving too many zeroes between the dollar-sign and the decimal.

Due to the eight years he spent teaching high school English to reluctant teenagers, Thomas eschews obfuscation whenever possible, and delights in reducing complex, convoluted Texas law to practical paradigms.

Outside of the office, Thomas maintains his sanity by riding a bicycle as fast as possible. Thomas has been signing his email messages with his initials since before Al Gore invented the internet, and he contains his mild exasperation that no one has yet started calling him Tag.

Let it Snowden!

Thomas A. Gwosdz
City Attorney
Victoria, Texas
(361) 485-3520
tgwosdz@victoriatx.org

Edward Snowden joined the CIA as a systems administrator and telecommunications systems officer in 2006. In 2007, the CIA stationed him in Geneva Switzerland, where he was responsible for maintaining computer network security. During his time in Switzerland, his supervisor may have suspected that Snowden attempted to obtain classified information not authorized to him.[1]

In 2009, Snowden began working for Dell, inside an NSA facility in Japan, as a systems administrator. Investigators later estimated that "most" of Snowden's released documents were acquired while working at Dell.[2] By March of 2013, Snowden had begun working for Booz Allen in Hawaii, but he had been working at the NSA facility in Hawaii for at least 12 months prior to beginning his Booz Allen position.

Snowden contacted journalists in late 2012. By May of 2013, Snowden was releasing confidential records to at least three journalists. In January of 2014, Snowden claimed that the NSA does not limit its data collection to national security issues, and accused the agency of industrial espionage.

In light of Snowden's disclosures, attorneys must balance their obligation to protect client information against their need to communicate that information in a digital age. This paper seeks to examine that balance.

Ethical Rules

> *(b) Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e) and (f), a lawyer shall not knowingly: (1) Reveal confidential information of a client or a former client to: (i) a person that the client has instructed is not to receive the information; or(ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm.*[3]

The information covered by Rule 1.05 is, of course, broader than the evidentiary privilege under Rule 503 of the Texas Rules of Evidence or of Rule 503 of the Texas Rules of Criminal Evidence. "'Confidential information' includes both "privileged information" and 'unprivileged client information.'" [4]

[1] Schmitt, Eric. "C.I.A. Warning on Snowden in '09 Said to Slip Through the Cracks." The New York Times. October 10, 2013. Retrieved on January 30, 2014.

[2] Suzanna Andrews, Bryan Burrough & Sarah Ellison (May 2014), "The Snowden Saga: A Shadowland of Secrets and Light" Vanity Fair

[3] Tex. R. Prof. Cond., Rule 1.05 "Confidentiality of Information."

[4] TX ST RPC Rule 1.05.

The Rules allow a lawyer to knowingly reveal confidential information in a few select instances, and differentiates between privileged confidential information, and unprivileged confidential information.

<u>Disclosure of Privileged Client Information</u>:

Privileged confidential information of the client can be revealed in the following eight situations described by subparagraph (c):

> (1) When the lawyer has been expressly authorized to do so in order to carry out the representation.(2) When the client consents after consultation.(3) To the client, the client's representatives, or the members, associates, and employees of the lawyer's firm, except when otherwise instructed by the client.(4) When the lawyer has reason to believe it is necessary to do so in order to comply with a court order, a Texas Disciplinary Rules of Professional Conduct, *or other law*.(5) To the extent reasonably necessary to enforce a claim or establish a defense on behalf of the lawyer in a controversy between the lawyer and the client.(6) To establish a defense to a criminal charge, civil claim or disciplinary complaint against the lawyer or the lawyer's associates based upon conduct involving the client or the representation of the client.(7) When the lawyer has reason to believe it is necessary to do so in order to prevent the client from committing a criminal or fraudulent act.(8) To the extent revelation reasonably appears necessary to rectify the consequences of a client's criminal or fraudulent act in the commission of which the lawyer's services had been used.[5]

For the purpose of this examination, the most interesting of those eight permissive disclosures is number 4, which allows the attorney to disclose privileged client information when the lawyer believes it is necessary to comply with "other law." While the Rule seems to contemplate intentional, knowing disclosure, one might wonder whether merely allowing communications to be intercepted by government spy initiatives complies with subparagraph (c)(4).

In 1974, the Professional ethics committee reviewed a request for opinion from an attorney who faced possible prosecution by the SEC for failure to disclose confidential information of a former client. Although the former client had asserted his privilege before the SEC, and demanded that the attorney protect his confidential information, the SEC threatened to name the attorney a respondent in the injunctive proceeding if the attorney continued to assert the attorney-client privilege on behalf of his former client.

The Ethics Committee's analysis of the facts upheld the attorney's obligation to protect confidential information, but included this scathing condemnation of the SEC's practices:

> The determination of whether to disclose or testify or not should not be determined by the S.E.C., but by a Court of law. In light of the

[5] TX ST RPC Rule 1.05(c).

> various circumstances and highly-involved questions, *A* should not be required to pick and choose which questions are covered by the privilege—which questions may be covered by the ethical considerations, and which questions to which he should make full answer.
>
> The method of approach exhibited by the S.E.C. in this instance, that is, to investigate a party by propounding questions to this attorney and then forcing the attorney to testify against his client, runs contra to the entire system of adversary jurisprudence known to the common law.

Nevertheless, the opinion does not offer any relief to the attorney. In the nine paragraphs of the opinion which follow the scathing quote above, the Committee asks thirteen hypothetical questions of its own before concluding:

> The posing of all of the questions here in above contained simply point up the impropriety of a tribunal calling a client's lawyer as a witness against the client. It places the lawyer in an impossible position. If such practice is permitted to continue, it could destroy the concept of attorney-client relations.

Of course, the 1974 opinion addressed a prior version of the Rules. A similar inquiry today may reach different conclusions. But the upshot of the opinion is clear. As improper as it may be for the SEC to put the attorney in such a predicament, the rules allow no escape.

My personal analysis of the rule leads me to conclude that only a very limited set of facts would result in an effective defense to violation of Rule 1.05. In order for the revelation of client information to be permitted under Rule 1.05(c)(4), the lawyer must conclude that the disclosure is *necessary* to comply with "other law." If other methods of communication would avoid such disclosure, I do not believe that the disclosure is necessary to comply. Of course, given the breadth of government oversight of electronic communications, an attorney may determine that no other alternative exists.

<u>**Disclosure of Unprivileged Client Information**</u>:

Unprivileged client information, on the other hand, may be revealed in a slightly broader set of situations described in subparagraph (d):

> (1) When impliedly authorized to do so in order to carry out the representation.(2) When the lawyer has reason to believe it is necessary to do so in order to:(i) carry out the representation effectively;(ii) defend the lawyer or the lawyer's employees or associates against a claim of wrongful conduct;(iii) respond to allegations in any proceeding concerning the lawyer's representation of the client; or(iv) prove the services rendered to a client, or the reasonable value thereof, or both, in an action against another person or organization responsible for the payment of the fee for services rendered to the client.[6]

[6] TX ST RPC Rule 1.05(d).

In Ethics Opinion 506 (1994), the Professional Ethics Committee reviewed a request by an attorney who wished to disclose client information to the Texas Workers' Compensation Commission for the purpose of claiming a fee. TWCC requires specific documentary evidence of the representation, in the form of a general description of the nature of each conference with his clients, and the attorney sought an opinion regarding disclosure of the documentary evidence.

The Ethics Committee determined that if the requested information involved a general description of the nature of conferences between the attorney and client and not a report of the substance of communications between the client and the attorney, the requested information will normally constitute confidential information that is not "privileged information." In addition to determining that the disclosure would be permitted under (d)(2)(iv) in an "action" for the payment of a fee for services, the Committee separately determined that:

> in the absence of special circumstances, such disclosure should normally be viewed as impliedly authorized in order to permit the attorney to carry out the representation. Hence disclosure would also normally be permitted by Rule 1.05(d)(1), which authorizes an attorney to disclose unprivileged information "[w]hen impliedly authorized to do so in order to carry out the representation."

While this opinion seems to broadly allow an attorney to disclose non-privileged information based on an undefined implication of authorization, it does turn tightly on the distinction between privileged and unprivileged information. Application of attorney-client privilege depends on whether communication sought to be protected is "confidential." A communication is "confidential" if it is not intended to be disclosed to third persons other than those to whom disclosure is made in furtherance of the rendition of professional legal services to the client. [7] The critical distinction is the matter of intent.

A "Venerable Rule" in Texas jurisprudence holds that, because the privilege protects only confidential communications, the presence of a third person ... eliminates the intent for confidentiality on which the privilege rests. The privilege is not, however, waived if a privileged communication is shared with a third person who has a common legal interest with respect to the subject matter of the communication. [8] Therefore, the Fifth Circuit has held that communication between attorney and client is protected by privilege if it is intended to remain confidential and was made under circumstances so that communication was reasonably expected and understood to be confidential.[9] That ruling, however, provides little guidance where a third party, the US Government, *might* be listening to an otherwise confidential communication.

To determine whether an expectation of privacy is reasonable, we must examine what we know about the NSA surveillance programs.

[7] *Williams v. State*, 417 S.W.3d 162, 186 (Tex. App.—Houston [1st Dist.] 2013, pet. ref'd)

[8] *In re Auclair*, 961 F.2d 65, 69 (5th Cir. 1992)

[9] *Id.*

NSA Programs

Five Eyes –

> *A "supra-national intelligence organization that doesn't answer to the laws of its own countries."*
>
> *-- Edward Snowden*

Five Eyes is an international alliance of Anglophonic countries, including Australia, Canada, New Zealand, the United Kingdom and the United States of America.[10] Five Eyes can be traced to the conclusion of World War II, when the Atlantic Charter laid out goals for a post-war world. During the Cold War, Five Eyes used the ECHELON surveillance system to monitor communications among Soviet Bloc countries.[11] In the 1990s, ECHELON's existence was revealed to the public, including revelations that it was used to monitor billions of private communications worldwide.[12] Since 2001, the Five Eyes have further expanded their surveillance capabilities, with much of the emphasis being placed on monitoring the internet.

Five Eyes is not a "program" in the same sense as the other programs disclosed by Edward Snowden. Nor was it secret before his disclosures. Rather, Edward Snowden described the Five Eyes as a "supra-national intelligence organisation that doesn't answer to the laws of its own countries,"[13] For the purpose of this paper, the Five Eyes are significant because they reportedly have been intentionally spying on one another's citizens and sharing the collected information with each other in order to circumvent restrictive domestic regulations on spying.[14] US domestic targets of the Five Eyes include Strom Thurmond,[15] and Jane Fonda.[16]

[10] The *Nine* Eyes consist of the Five Eyes plus Denmark, France, the Netherlands and Norway. The *Fourteen* Eyes consist of the Nine Eyes plus Germany, Belgium, Italy, Spain and Sweden. According to Edward Snowden, the Fourteen Eyes are officially known as SIGINT Seniors Europe, or "SSEUR."

[11] Asser, Martin (6 July 2000). "Echelon: Big brother without a cause?". BBC. Retrieved 28 January 2014.

[12] "Q&A: What you need to know about Echelon". BBC. 29 May 2001. Retrieved 28 January 2014.

[13] "Snowden-Interview: Transcript". Norddeutscher Rundfunk. 26 January 2014. Retrieved 28 January 2014.

[14] Ball, James (20 November 2013). "US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data". The Guardian. Retrieved 18 January 2014. MacAskill, Ewen (2 December 2013). "Revealed: Australian spy agency offered to share data about ordinary citizens". The Guardian. Retrieved 18 January 2014.

[15] In 1988, Margaret Newsham, a Lockheed employee, told a closed-door session of the United States Congress that Thurmond's telephone calls were being intercepted by the Five Eyes via their ECHELON surveillance system. Campbell, Duncan (25 July 2000). "Inside Echelon". Heise Online. Retrieved 19 January 2014.

[16] Due to her political activism, her communications as well as those of her husband, Tom Hayden, were intercepted by the GCHQ and handed over to the NSA. Hanson, Christopher (13 August 1982). "British 'helped U.S. in spying on activists'". The Vancouver Sun. Retrieved 30 November 2013.

PRISM –

> *"…in general, the reality is this: if an NSA, FBI, CIA, DIA, etc. analyst has access to query raw SIGINT [signals intelligence] databases, they can enter and get results for anything they want."*
>
> *-- Edward Snowden*

PRISM is an NSA intelligence program that grew out of the 1970's Terrorist Surveillance Program. As implemented under the George W. Bush administration in response to the September 11 terrorist attacks, PRISM was criticized by the American Bar Association, among others, as being potentially unconstitutional.[17] PRISM was later enabled by the Protect America Act of 2007, and expanded to include limited warrantless monitoring of international terror suspects by the FISA Amendments Act of 2008.

Under the PRISM program, NSA likely could unilaterally access data and perform "extensive, in-depth surveillance on live communications and stored information" with examples including email, video and voice chat, videos, photos, voice-over-IP chats (such as Skype), file transfers, and social networking details.[18] At least some of these services would be unaffected by encrypting messages, because PRISM collected data prior to encryption.[19] Although PRISM is directed toward international terrorists, it collects data on communications among people with up to three degrees of separation from the suspected terrorist.[20] Because the broadly collected data was stored by the NSA, analysts could search the database and listen to calls, or read information from any of those people without further warrants.

XKeyscore –

> *"You could read anyone's email in the world, anybody you've got an email address for. Any website: You can watch traffic to and from it. Any computer that an individual sits at: You can watch it. Any laptop that you're tracking: you can follow it as it moves from place to place throughout the world. It's a one-stop-shop for access to the NSA's information."*
>
> *-- Edward Snowden*

[17] "Adopted by the House of Delegates" (PDF). American Bar Association. February 13, 2006.

[18] Greenwald, Glenn; MacAskill, Ewen (June 6, 2013). "NSA Taps in to Internet Giants' Systems to Mine User Data, Secret Files Reveal – Top-Secret Prism Program Claims Direct Access to Servers of Firms Including Google, Apple and Facebook – Companies Deny Any Knowledge of Program in Operation Since 2007 – Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks". The Guardian. Retrieved June 15, 2013.

[19] Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman and Dominic Rushe (July 11, 2013). "Revealed: how Microsoft handed the NSA access to encrypted messages". The Guardian. Retrieved July 11, 2013.

[20] Ackermann, Spencer (17 July 2013). "NSA warned to rein in surveillance as agency reveals even greater scope". The Guardian. Retrieved July 18, 2013. Bump, Philip (17 July 2013). "The NSA Admits It Analyzes More People's Data Than Previously Revealed". The Atlantic Wire. Retrieved July 18, 2013. Watkins, Aiy (17 July 2013). "Skeptical Congress turns its spycam on NSA surveillance". McClatchy News Service. Retrieved July 18, 2013.

XKeyscore or XKEYSCORE (abbreviated as XKS) is a formerly secret computer system first used by the United States National Security Agency for searching and analyzing Internet data it collects worldwide every day. Snowden describes XKeyscore as a "front end search engine."[21]

XKeyscore consists of over 700 servers at approximately 150 sites where the NSA collects data, including "US and allied military and other facilities as well as US embassies and consulates" in many countries around the world.[22] From these sources, XKeyscore stores "full-take data", which are indexed by plug-ins that extract certain types of metadata (like phone numbers, e-mail addresses, log-ins, and user activity) and index them in metadata tables, which can be queried by analysts.[23]

Because XKeyscore holds raw and unselected communications traffic, analysts can not only perform queries using "strong selectors" like e-mail addresses, but also using "soft selectors", like keywords, against the body texts of e-mail and chat messages and digital documents and spreadsheets in English, Arabic and Chinese.[24] However, because of the sheer volume of data collected by XKeyscore, (20+ terabytes/day in 2008) the raw data can sometimes only be held for three to five days. Metadata extracted from the raw data can be kept as long as 30 days.

The deep analysis of data permitted by XKeyscore allows analysts to accomplish tasks not possible with other analytical tools. For example, XKeyscore can detect the nationality of foreigners by analyzing the language used within intercepted emails, like finding a German speaker in Pakistan. It can show the usage of Virtual Private Networks (VPNs); it can track the source and author of a document that has been shared by many people. In 2008, NSA planned to add new capabilities, including VOIP.[25]

<u>Tempora</u> –

> *"It's not just a U.S. problem. The UK has a huge dog in this fight...They [GCHQ] are worse than the U.S."*[26]
>
> *-- Edward Snowden*

Tempora is a clandestine security electronic surveillance program tested in 2008, established in 2011 and operated by the British Government Communications Headquarters (GCHQ).[27] Tempora uses intercepts on the fibre-optic cables that make up

[21] "Snowden Interview Transcript". Norddeutscher Rundfunk. Retrieved 27 January 2014.

[22] Staff (undated; circa July 2013). "No alvo dos EUA – O big-brother na América Latina e no mundo" [The U.S. Targets – Big Brother in Latin America and in the World]. O Globo (in Portuguese). Retrieved August 5, 2013.

[23] Staff (July 31, 2013). "XKeyscore Presentation from 2008 – Read in Full". The Guardian. Retrieved August 6, 2013.

[24] *Id.*

[25] *Id.*

[26] Ewen MacAskill; Julian Borger; Nick Hopkins; Nick Davies; James Ball (21 June 2013). "GCHQ taps fibre-optic cables for secret access to world's communications". The Guardian (London). Retrieved 21 June 2013.

[27] Shubber, Kadhim. "A simple guide to GCHQ's internet surveillance program Tempora". Wired. Retrieved 25 June 2013.

the backbone of the internet to gain access to large amounts of internet users' personal data. The intercepts are placed in the United Kingdom and overseas, with the knowledge of companies owning either the cables or landing stations.[28] Using Tempora, GCHQ potentially has access to 21 petabytes of data each day.[29]

Tempora is said to gather recordings of telephone calls, the content of email messages, Facebook entries, and the personal internet history of users. News articles about Tempora claim that no distinction is made in the gathering of data between private citizens and targeted suspects.[30] *Wired*, the online news magazine, describes the process GCHQ uses to analyze the data:

> They use a technique called Massive Volume Reduction (MVR). Peer-to-peer downloads, for example, are classed as "high-volume, low-value traffic" and discarded by an initial filter. This reduces the volume of data by 30 percent. They use specific searches, which can relate to trigger words, email addresses of interest, or targeted persons and phone numbers. GCHQ and the NSA have identified 40,000 and 30,000 triggers respectively.[31]

GCHQ maintains that British law legitimizes the operation of Tempora. The 2000 Regulation of Investigatory Powers Act (RIPA) permits the tapping of defined targets when authorized by a warrant signed by the home secretary or foreign secretary. In addition, RIPA also allows the foreign secretary to sign a certificate for the interception of broad categories of material, as long as one end of the monitored communications is abroad. The nature of modern fibre-optic communications means that a proportion of internal UK traffic is relayed abroad and then returns through the cables, thereby falling within the ambit of RIPA.[32]

<u>Muscular</u> –

Muscular is a surveillance program operated jointly by the US NSA and British GCHQ. Using Muscular, GCHQ and NSA have secretly broken into the main communications links that connect large data centers around the works, and are able to acquisition internal Yahoo! and Google unencrypted data.[33] To stay current, these data centers must synchronize large volumes of information about account holders. Yahoo's

[28] Ball, James (25 October 2013). "Leaked memos reveal GCHQ efforts to keep mass surveillance secret". The Guardian. Retrieved 25 October 2013.

[29] Shubber, Kadhim. "A simple guide to GCHQ's internet surveillance program Tempora". Wired. Retrieved 25 June 2013.

[30] Ewen MacAskill; Julian Borger; Nick Hopkins; Nick Davies; James Ball (21 June 2013). "GCHQ taps fibre-optic cables for secret access to world's communications". The Guardian (London). Retrieved 21 June 2013

[31] Shubber, Kadhim. "A simple guide to GCHQ's internet surveillance program Tempora". Wired. Retrieved 15 May 2014.

[32] Ewen MacAskill; Julian Borger; Nick Hopkins; Nick Davies; James Ball (21 June 2013). "GCHQ taps fibre-optic cables for secret access to world's communications". The Guardian (London). Retrieved 15 May 2014.

[33] Gellman, Barton; Soltani, Ashkan (October 30, 2013). "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". The Washington Post. Retrieved 15 May 2014.

internal network, for example, sometimes transmits entire e-mail archives — years of messages and attachments — from one data center to another.[34] Tapping into those data centers allows the NSA to intercept unencrypted communications in real time and to take a retrospective look at target activity.

According to the Washington Post, the Muscular program collects more than twice as many data points (“selectors” in NSA jargon) compared to the better known PRISM.[35] In one 30-day period, Muscular was able to collect over 181 million records.[36]

The existence of Muscular’s back-door access is interesting, given that NSA has front-door access to similar information through court-approved warrants in the PRISM program.

Muscular collects data from an access point outside the United States, and relays the data to the NSA at Fort Meade, Maryland.[37] The collection relies on the fact that (at the time at least) data was transmitted unencrypted inside Google's private cloud, with "Google Fronted Servers" stripping and respectively adding back SSL from/to external connections. After the information about MUSCULAR was published by the press, Google announced that it was working on deploying encrypted communication between its datacenters.[38]

[34] *Id.*

[35] *Id.*

[36] Gellman, Barton; DeLong, Matt (2013-10-30). "One month, hundreds of millions of records collected". The Washington Post. Retrieved 2014-01-27. As large as Muscular is purported to be, it is claimed to be dwarfed by another program, called INCENSER, which collected over 14 billion records in the same period.

[37] Gellman, Barton; DeLong, Matt. "How the NSA's MUSCULAR program collects too much data from Yahoo and Google". The Washington Post. Retrieved 28 December 2013.

[38] Gellman, Barton; Soltani, Ashkan (October 30, 2013). "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say". The Washington Post. Retrieved October 31, 2013.