January 18, 2001

THE SEARCH & SEIZURE OF ELECTRONIC INFORMATION: THE LAW BEFORE AND AFTER THE USA PATRIOT ACT[1]

*Changes made by the USA PATRIOT Act appear **in bold**.

TYPE OF INFORMATION SOUGHT	How Can Government Authorities Compel Disclosure?				Can An Organization Make A Voluntary Disclosure To Government Authorities?	
	Type Of Legal Process[2]	Standard To Be Met Before Issuance	How Issued	How Is Information Used	Public Provider[3]	Non-Public Provider
Basic subscriber information (*e.g.* name, address, billing records, telephone number, length of service, type of service, **payment information**, **session times and duration, network addresses**)	Subpoena [18 USC § 2703(c)]	Relevant to investigation	Signed by prosecutor (if grand jury) or by agent (if administrative)	Criminal and administrative investigations; **to any other Federal official if consistent with "foreign intelligence exception"[4]**	No [18 USC § 2702] (but other exceptions apply, including **emergency where provider reasonably believes there is immediate danger of death or serious physical injury ("emergency exception")[5]**	No [18 USC § 2702] (but other exceptions apply, including **emergency exception**)
	Court order [18 USC § 2703(d)]	Specific and articulable facts	Court issues order upon government showing that meets standard	Criminal investigations; **foreign intelligence exception**		
	Search warrant [18 USC § 2703(c)(1)(C)]	Probable Cause	Court issues warrant upon application supported by affidavit **(nationwide execution)**	Criminal investigations; **foreign intelligence exception**		
	FISA order (subpoena) [50 USC § 1862]	**Business records related to terrorism or clandestine intelligence activities[6]**	By secret FISA court upon application by FBI	Intelligence investigations		

TYPE OF INFORMATION SOUGHT	How Can Government Authorities Compel Disclosure?				Can An Organization Make A Voluntary Disclosure To Government Authorities?	
	Type Of Legal Process[2]	Standard To Be Met Before Issuance	How Issued	How Is Information Used	Public Provider[3]	Non-Public Provider
Transaction and account records	Court order [18 USC § 2703(d)]	Specific and articulable facts	Court issues order upon government showing that meets standard	Criminal investigations; **foreign intelligence exception**	No [18 USC § 2702] (but exceptions apply, including consent and **emergency exception**)	No [18 USC § 2702] (but exceptions apply, including consent and **emergency exception**)
	Search warrant [18 USC § 2703(c)(1)(B)]	Probable Cause	Court issues warrant upon application supported by affidavit **(nationwide execution)**	Criminal investigations; **foreign intelligence exception**		
	FISA order (subpoena) [50 USC § 1862]	**Business records related to terrorism or clandestine intelligence activities**	By secret FISA court upon application by FBI	Intelligence investigations		
E-mail not opened by user that has been in electronic storage *less than* 180 days	Search warrant [18 USC § 2703(a)]	Probable Cause	Court issues warrant upon application supported by affidavit **(nationwide execution)**	Criminal investigations; **foreign intelligence exception**	No [18 USC § 2702(a)(1)] (but exceptions apply including **emergency exception**)	Yes [18 USC § 2702(a)(1)]
E-mail not opened by user that has been in electronic storage *more than* 180 days	Subpoena with notice to target	Relevant to investigation	Signed by prosecutor (if grand jury) or by agent (if administrative)	Criminal and admin. investigations; **foreign intelligence exception**	No [18 USC § 2702(a)(1)] (but exceptions apply including **emergency exception**)	Yes [18 USC § 2702(a)(1)]
	Court order with notice to target [18 USC § 2703(d)]	Specific and articulable facts	Court issues order upon government showing that meets standard	Criminal investigations; **foreign intelligence exception**		
	Search warrant [18 USC § 2703(a) & (b)]	Probable Cause	Court issues warrant upon application supported by affidavit **(nationwide execution)**	Criminal investigations; **foreign intelligence exception**		

TYPE OF INFORMATION SOUGHT	How Can Government Authorities Compel Disclosure?				Can An Organization Make A Voluntary Disclosure To Government Authorities?	
	Type Of Legal Process[2]	Standard To Be Met Before Issuance	How Issued	How Is Information Used	Public Provider[3]	Non-Public Provider
E-mail that *has* been opened by the user	Subpoena with notice to target	Relevant to investigation	Signed by prosecutor (if grand jury) or by agent (if administrative)	Criminal and admin. investigations; **foreign intelligence exception**	No [18 USC § 2702(a)(2)] (but exceptions apply including **emergency exception**)	Yes [18 USC § 2702(a)(2) and § 2711(2)]
	Court order with notice to target	Specific and articulable facts	Court issues order upon government showing that meets standard	Criminal investigations; **foreign intelligence exception**		
	Search warrant [18 USC § 2703(b) & 18 USC § 2705]	Probable Cause	Court issues warrant upon application supported by affidavit **(nationwide execution)**	Criminal investigations; **foreign intelligence exception**		
Stored voice-mails that were transmitted *via* computer	**Search warrant** [18 USC § 703(b)]	Probable Cause	Court issues warrant upon application supported by affidavit **(nationwide execution)**	Criminal investigations; **foreign intelligence exception**	No [18 USC § 2702(a)(1)] (but exceptions apply including **emergency exception**)	Yes [18 USC § 2702(a)(1)]
	Wiretap order [18 USC § 2516(1)]	Probable cause that target committed one of list of serious crimes **(including terrorism and computer crimes)**	Court issues warrant upon application supported by affidavit	Criminal investigations; **foreign intelligence exception**		

TYPE OF INFORMATION SOUGHT	How Can Government Authorities Compel Disclosure?				Can An Organization Make A Voluntary Disclosure To Government Authorities?	
	Type Of Legal Process[2]	Standard To Be Met Before Issuance	How Issued	How Is Information Used	Public Provider[3]	Non-Public Provider
Real-time interception of *non-content* information (including **dialing, routing, addressing, signaling information, IP addresses and port numbers, "to" and "from" information in e-mail header**)	Pen/Trap Order [18 USC § 3122]	Relevant to a criminal investigation	Court issues order upon government showing that meets standard **(nationwide execution) (device can now be placed on computer)**	Criminal investigations; **foreign intelligence exception**	No [18 USC § 3121] (but exceptions apply)	No [18 USC § 3121] (but exceptions apply)
	FISA order (pen/trap) [50 USC § 1842(c)]	**Concern foreign intelligence, do not concern a U.S. citizen, or do concern U.S. citizen and protect against terrorism or intelligence activities**	By secret FISA court upon application by Attorney General	Foreign intelligence investigations		
Real-time interception of electronic communications (content)	Wiretap order [18 USC § 2516(1)]	Probable cause that target committed one of list of serious crimes **(including terrorism and computer crimes)**	Court issues warrant upon application supported by affidavit	Criminal investigations; **foreign intelligence exception**	No [18 USC § 2511(2)(i)] (but exceptions apply, including **where provider has reasonable grounds to believe that target is computer trespasser**)	No [18 USC § 2511(2)(i)] (but exceptions apply, including **where provider has reasonable grounds to believe that target is computer trespasser**)
	FISA order (wiretap) [50 USC § 1805]	Target is foreign agent and **a significant purpose is to gather foreign intelligence**	By secret FISA court upon application by Attorney General **(can be executed on any phone or computer used by target)**	Foreign intelligence investigations		

The information provided in this chart is not intended to provide legal guidance on the application of the statutes cited to any specific factual situation. Please consult with counsel in order to ensure compliance with applicable law, policies and procedures.

---

[1] The USA Patriot Act, Pub. L. No. 107-56 (2001), makes changes to over fifteen (15) different statutes. Among those statutes changed or modified are the Electronic Communications Private Act of 1986 (ECPA), 18 U.S.C. § 2801 et. seq., the Computer Fraud and Abuse Act (CFFA), 18 U.S.C. § 1030, the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 et. seq., the Family Education Rights and Private Act (FERPA), 20 U.S.C. 1232(g), the Cable Act, 47 U.S.C. § 551, the Federal Wiretap Statute, 18 U.S.C. § 2510 et. seq., and the Federal Rules of Criminal Procedure.

[2] United States law sets forth the type of legal process required before a government authority may compel the production of information from a private individual or organization, as well as the standard that the government must meet before obtaining such process. As a general matter, the more "private" the type of information, the higher the standard the government must meet in order to compel production. The types of legal process discussed here are as follows: (1) a subpoena is a document that compels the production of tangible things. It can be issued by an official in connection with a grand jury investigation. In addition, certain federal agencies have the authority to issue administrative subpoenas in connection with investigations under their authority; (2) a search warrant, which authorizes the search of physical premises and seizure of tangible items, is issued by a court upon a showing of probable cause; (3) pen register and trap-and-trace device court orders authorize the collection of telephone and computer identifying information dialed to and from a particular communications device; (4) a wiretap order, also issued by a court, authorizes the real-time interception of communications. Such orders require an affidavit setting forth detailed information and establishing probable cause that the target committed one of a list of specified serious crimes; and (5) FISA orders are issued by a secret FISA court, and allow the compulsion of information, under very strict procedures, in search of information that relates to foreign intelligence and counter-intelligence.

[3] If a provider does not provide services "to the public," then the ECPA does not place any restrictions on the disclosure of the contents. *See* 18 U.S.C. § 2702(a). Whether a university or library is a public or private provider will involve a fact-specific determination.

[4] The USA Patriot Act added broad new information sharing authority that pertains to previously confidential information including grand jury information and intercepted communications. Section 203(b) permits sharing of any information lawfully obtained by a law enforcement official. The officer may disclose the contents of such communications to any other federal law enforcement official who is to receive the information to perform his official duties "to the extent such contents include foreign intelligence or counterintelligence or foreign intelligence information." In addition, Section 504 of the Act authorizes general coordination between law enforcement and FISA surveillance.

[5] These exceptions permit disclosure: (1) to an addressee or intended recipient of the communication or their agent; (2) as otherwise authorized in sections 2517, 2511(2)(a), or 2703 of Title 18; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computer service; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or (6) to a law enforcement agency if the contents were inadvertently obtained by the provider and appear to pertain to the commission of a crime; or if required by section 227 of the Crime Control Act of 1990. The USA PATRIOT Act, section 212, adds an exception and permits disclosures to law enforcement "if the emergency provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information."

[6] Previously, FISA authorized collection of business records in very limited situations, mainly records relating to common carriers, vehicles or travel, and only via court order. The USA PATRIOT Act substantially expands this collection to all "tangible things," including business records, that may be obtained via a subpoena.