ELECTRONIC FRONTIER FOUNDATION

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	twitter	facebook	facebook	facebook
Date	**Updated**	**2008**	**2009**	**2010**
Date, length, link (if available) and other info	Available on Twitter site at: http://support.twitter.com/entries/41949-guidelines-for-law-enforcement	February 2008, five pages	2009, 11 pages	May 2010, 5 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	Addresses but does not distinguish: "We require a subpoena, court order, or other valid legal process to disclose information about our users." By default, most Twitter profile information is public. This includes, according to the privacy policy, name and username. It also may include a short bio, cell phone number, location, address book, a picture, "the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information." "Non-public information about Twitter users is not released unless we have received a subpoena, court order, or other valid legal process document."	Does not say	• Subpoena for non-content (basic subscriber info), • ECPA 2703(d) order for limited content (e.g. messages over 180 days), • search warrant for remaining content (p. 3)	"we will provide records as required by law." (p.2)
How does site define and/or distinguish different types of user information	Law Enforcement Guide, TOS & Privacy Policy only distinguish between public and non-public information	Does not distinguish between basic subscriber information and other information (p. 4)	User ID number, email address, time account was created, most recent logins, registered mobile number, whether account is publicly viewable (p. 6) "User Neoprint": Contact information, mini-feed, status update history, shares, notes, wall posts, friend listings (including their IDs), group listings (including group member IDs), future and past events, video listings (p. 6)	User ID number, email address, date/time account was created, most recent logins, registered mobile number (p. 4) "Expanded Subscriber Content (sometimes referred to as Neoprint)": Contact information, mini-feed, status update history, shares, notes, wall postings, friend listings (include friend IDs), group listings (including group member IDs), future and past events, video listings (p. 4)
What other info is available?	Twitter does not host any content other than tweets. This includes any video or images that users may share through their accounts.	User photos, group contact information (p. 4)	"User Photoprint": User uploaded photos and photos tagged with user's name, group contact information, private messages (p. 7)	"User photos (sometimes referred to as User Photoprint)": User uploaded photos and photos tagged with user's name, group information, private messages (p. 4)
How does LE Guide address IP and other logs?	Twitter's servers automatically record information ("Log Data"), which may include information such as IP address, browser type, the referring domain, pages visited, and search terms. Other actions, such as interactions with advertisements, may also be included in Log Data.	• Logs are available and include: Script - script executed, Scriptget - additional information passed to the script, Userid - Facebook user id of the account active for the request, View time - date of execution in Pacific Time, IP - source address	• now have a limited capacity of retrieving specific logs and are technically limited in providing "everything" within a requested date range. We are unable to testify to the completeness of the data. • Logs include same data as 2008 • IP logs contain content and are treated as such under ECPA (p. 7)	• IP logs contain same data as 2008/09 and also include Session Cookie -- HTTP cookie set by user session • Logs are often incomplete, but if available will be provided (p. 4)
How long is data generally retained? How long in reponse to preservation request?	"Twitter retains different types of information for different time periods. Given Twitter's real-time nature, some information may only be stored for a very brief period of time."	90 days (page 3), though IP data may be retained shorter or longer depending (p. 5)	90 days, but an extension can be made if necessary (p. 6)	90 days, but an extension can be made if necessary. "By default we will return data no older than 90 days prior to the date we receive the request." (p. 2)
Is content that has been changed or deleted by user (including private messages) still available?	unclear	Content available as long as not deleted by user (page 4)	• If user has saved messages, they can be recovered. If deleted by user, they cannot be recovered (page 7) • If a profile is changed or updated, deleted content is not retained (page 6)	If messages are retained by user, they are available (page 4)
Can law enforcement monitor user account without user knowledge?	"Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order."	Does not say	Will normally disable account unless law enforcement clearly specify that doing so will hurt investigation (page 5)	Will normally disable account unless law enforcement clearly specify that doing so will hurt investigation (page 2)
Does site have exception for emergency disclosure?	Does not say.	Does not say	Can provide upon answering 3 questions: Describe emergency? Provide ID of users involved? Provide location of evidence? (pp. 8, 10)	Can provide upon answering 3 questions:Describe emergency? Provide ID of users involved? Provide location of evidence? (p. 5)
Does site charge law enforcement fees?	Does not say.	Reserves right to charge reasonable fees (p. 2)	Reserves the right to charge reasonable fees (p. 5)	Does not say
What are the requirements to begin preserving records?	"Preservation requests must be signed, include a valid return email address, and sent on law enforcement letterhead."	Request to preserve that includes law enforcement officer ID, contact informtion, name of agency (p. 3)	Request to preserve from law enforcement with ID, name of agency, and contact info (p. 5)	Request to preserve from law enforcement, with ID, name of agency, and contact info (p. 3)
Does site address fake accounts created by law enforcement?	Not addressed specifically, but Twitter acknowleges that users may create fake or anonymous profiles However, Twitter's "Rules" prohibit impersonation: "You may not impersonate others through the Twitter service in a manner that does or is intended to mislead, confuse, or deceive others"	Will disable accounts that violate terms of service, including fake police accounts (p. 2)	Will disable fake police accounts (p. 3)	Will "always disable accounts that supply false or misleading profile information or attempt to technically or socially circumvent site privacy measures." (p. 2)
Can user consent to data release?	Yes - Twitter may "share or disclose your information with your consent, such as when you use a third party web client to access your Twitter account"	Does not say	Will release data upon user consenting through form (pp. 8, 11)	Does not say
How will site deliver data?	Does not say.	Generally through email (p. 3)	Generally through email (p. 5)	Does not say
Other info?	N/A	Facebook may be able to retrieve specific information not described in guide (p. 5)	"Special Requests": Facebook may be able to retrieve specific information not described in guide (p. 9)	"We are required to disable accounts engaged in illegal activity, even if that activity is brought to our attention through a request for records." (p.5)
Sample forms or sample language?	N/A	N/A	Emergency Disclosure Form, User Consent to Release Form	Emergency Disclosure Form

	myspace	myspace.com	myspace.com	myspace.com	msn	msn
Date	**2005**	**March 2006**	**June 2006**	**2007**	**2006**	**2008**
Date, length, link (if available) and other info	September 2, 2005, 7 pages	March 13, 2006, 16 pages	June 23, 2006, 16 pages	November 1, 2007, 15 pages	July 2006, 2 pages	March 2008, 22 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	• Most profile information is publicly viewable and available. Publicly available information includes journal entries (in most cases), images, user comments, and public profile information." (p.2) • MS requires a subpoena for following info: -IP logs (recorded at time of login), Dates and times of login (PST), Email address, ZIP code, name, private messages (pp.2-3)	"Most profile information is publicly viewable and available." (Guide includes instructions for law enforcement to download this info) • Non-public information requires subpoena, search warrant, or other legal process • Non-public info includes: IP logs (recorded at time of login), Date profile created, Dates and times of login, E-mail address, ZIP code, Name, Private Messages, Private blogs (some info may not be accurate) (p. 6) • Information provided in response to subpoena: email address, IP Logs, private messages (p.10)	MySpace is both an ECS and RCS (p.4) • *subpoena* for "basic user identity, log-in information, and stored files", • *§ 2703(d) court order* for "user's date of birth, gender, hometown, and occupation, as well as historical private message header information." • *search warrant* for private user communications less than 180 days old. • *Subpoena or court order with prior notice to the subscriber (or delayed notice under 18 U.S.C. § 2705)* for Stored user files (photos, videos, blogs, classifieds, messages posted on forums or groups, address book and calendar contents) • *pen register/trap and trace order* for ongoing information about user's IP address each time they log-in to their account (pp. 4-7) • Law enforcement can obtain publicly available info without MySpace's assistance. (p. 4,5)	"Depending on the type of information sought, ECPA may require the use of a different form of legal process, and the period MySpace retains the information may differ." (p. 4) • subpoena or § 2703(c)(2) demand for "Basic user identity information," including "date profile created; first and last name provided by user; user ID; e-mail address provided by user; ZIP code, city, and country provided by user; account creation date and time; and the IP address at the time of sign-up." • subpoena or § 2703(c)(2) demand for historical "logs showing the IP address assigned to the user and the date stamp at the time the user accessed his or her profile." • Pen register/trap and trace order to "caputre log-in IPs prospectively." • Search warrant for messages less than 180 days old. • Subpoena or court order (or delayed notice under 18 U.S.C. § 2705) for messages over 180 days old. • Subpoena, civil investigative demand, or court order for "profile information including photos, videos, blogs, blog comments by other users, the identities fo the friends and 'About Me' entries." • § 2703(d) court order for "user's date of birth, gender, hometown, and occupation, as well as historical private message header information, excluding subject."(pp. 5-6)	ECPA "governs what legal documentation is required in order for Microsoft's Online Service records custodian to disclose customer account information and email content." • *subpoena* for basic subscriber information, including "name address, length of service (start date), screen names, other email accounts, IP address/IP logs/Usage logs, billing information, and e-mail content greater than 180 days old as long as the governmental entity follows the customer notification provisions in ECPA (see 18 U.S.C. § 2705)." (p. 2) • *2703(d) order* "will compel disclosure of all of the Basic Subscriber information available under a sbupoena plus the Address Book, Buddy Lists, the rest of a customer's profile not already listed above, internet usage logs (WEBTV), e-mail header information (to/from) excluding subject line, and e-mail content greater than 180 days old as long as the governmental entity follows the customer notifications provisions of ECPA (see 18 U.S.C. § 2705)." (p. 2) • *search warrant* is required for all email content under 180 days (p. 2)	ECPA "sets forth the appropriate legal process required to compel Microsoft's Online Service Records Custodians to disclose customer records and contents" • *subpoena* for basic subscriber information, including "name, address, length of service (start date), screen names, other email acounts, IP address/IP logs/Usage logs, billing information content (other than e-mail, such as Windows Live Spaces and MSN Groups) and e-mail content more than 180 days old as long as the governmental entity follows the customer notification provisions in ECPA (see 18 U.S.C. §§ 2703(b), 2705) • *2703(d) order* "will compel disclosure of all of the basic subscriber information available under a subpoena pluse the e-mail address book, Messenger contact lists, the rest of a customer's profile not alread listed above, internet usage logs (e.g. WEBTV or MSN Internet Access), and e-mail header information (to/from) excluding subject line." • *Search warrant* "will compel disclosure of all information available with a court order issued pursuant to 2703(d) (as listed above), plus all contents (if prior notice is not provided or an order for delayed notice is not obtained), and is the only means to compel the disclosure of e-mails, including subject line, in electronic storage 180 days or less."(p. 22) • "as Microsoft receives and processes legal process for its online services in the Ninth Circuit, [pursuant to *Theofel et al v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003)]Microsoft discloses both opened and unopened e-mail in electronic storage for 181 days or less only upon pursuant to a search warrant.
How does site define and/or distinguish different types of user information	Guide only distinguishes between public and non-public information (p.2)	Guide only distinguishes between public and non-public information (p. 6)	basic "user" ID info including user's name, email address, ZIP code, city & country, account creation date/time, IP address at time of signup -- all available via subpoena (pp. 6-7) user's birthday, gender, hometown, occupation, private message header information; search warrant: messages less than 180 days old -- all available via court order: (p. 6)	Basic user ID (subpoena): date profile created, name, user ID, email address, ZIP code, city, county, account creation date, IP address; other (court order) IP logs, birthday (pp. 5-6) Search warrant: private messages less than 180 days old (p. 5)	Basic (subpoena): name, address, length of service, screen names, IP address, IP logs, billing info, email greater than 180 days (p. 2) Full profile (court order): address book, buddy list, email header info, email content great than 180 days; Email (warrant): all messages less than 180 days old (p. 2)	Basic (subpoena): name, address, length of service, screen names, IP address, IP logs, billing info, email greater than 180 days (p. 22) Full profile (court order): address book, buddy list, email header info, email content great than 180 days; Email (warrant): all messages less than 180 days old (p. 22)
What other info is available?	unclear	Unclear whether photos and other content are released (p. 6)	Photos, videos, blogs, classifieds can be disclosed with a subpoena (pages 6-7)	Photos, videos, blogs available with subpoena or court order (p. 6)	MSN groups and spaces are considered public, and will be disclosed with subpoena (p. 2)	Can get this information from all of MSN services, such as Xbox Live, Windows Live, etc. (p. 4)
How does LE Guide address IP and other logs?	IP Logs are available for up to ninety days after a user's last login.(p.3)	Available through subpoena. Info includes time and date stamp (p. 10)	Can be produced with subpoena (p. 6) Info includes IP address, date and time of log-in at time user accesses profile. Historic IP logs are available, and MySpace can capture IP logs prospectively with Pen/Trap order.	Can be produced with court order (p. 5)	Can be produced with subpoena (p. 2)	Can be produced with subpoena (p. 22)
How long is data generally retained? How long in reponse to preservation request?	• IP Logs are available for up to ninety days after a user's last login. • Private Messages in an active account User's Inbox - Retained until user removes them. • Sent Mail - Retained for 14 days. • Trash Mail - Retained 30 days or less. Users can empty their trash at any time. • Deleted Accounts - No mail is available for deleted accounts. • User ID, IP Address, Login date stamps are retained for up to 90 days after account • Profile information is available for up to ten days after account deletion.(p. 3)	• "MySpace does not retain information that is altered on or removed from an active profile. Once a change is made, existing information is overwritten." (p.7) • MySpace has different retention times for different types of info but law enforcement can request preservation for longer (p. 8) • Messages retained as long as not deleted; sent mail retained for 14 days; trash mail retained 30 days or less unless user empties trash, which permanently deletes message (p. 7)	• Messages retained as long as not deleted; sent mail retained for 14 days; trash mail retained 30 days or less unless user empties trash, which permanently deletes message (page 7) • Law enforcement can request preservation for longer (p.7) • Pursuant to preservation request: 90 days but can be extended an extra 90 (p. 8)	• Messages retained as long as not deleted; sent mail retained for 14 days; trash mail retained 30 days or less unless user empties trash, which permanently deletes message (page 7) • "MySpace honors all law enforcement preservation requests made during the period the data is available. MySpace also automatically preserves the data of users who are identified as registerd sex offenders and removed from the MySpace site pursuant to MySpace's Sentinel SAFE Project." (p.6) • Pursuant to preservation request: "MySpace will preserve the specific information identified in the request for up to 180 days and will extend the preservation as necessary at your request." (p. 8)	90 days from date of request, but can preserve for up to 270 days (p. 2)	90 days from date of request, but can preserve for up to 270 days (p. 22)
Is content that has been changed or deleted by user (including private messages) still available?	• MS cannot recover deleted messages unless it is in another user's Sent Mail; • "MySpace.com does not retain information that is altered/ removed on an active profile. Once a change is made, existing information is overwritten." (p.3)	• Myspace doesn't retain altered or removed info. However, MySpace may be able to retreive deleted messages from another user who sent or received email. User ID, IP Address, Login date stamps are retained for up to 90 days after account deletion. Profile information is available for up to ten days after account deletion. (p. 7)	User can delete and modify account (p.8) If user deletes account: • "User identity and date in the user profile is generally available for up to 10 days after account deletion. Other stored files, such as photos, may be lost at the time of account deletion." • "User ID, IP Address and Login date stamps are retained for up to 90 days after account deletion. • no mail is available for deleted accounts (p.8)	User can delete and modify (p. 6) • "Upon receipt of a preservation request, however, MySpace will capture all user data available at that time, and future actions by the user will not affect the preserved data."(p. 6) • "User identity information is available for one year after account deletion. Other stored files, such as photos, may be lost at the time of account deletion." • "MySpace retains Friend ID, IP Address and Login time and date stamps dating back one year." • "No private messages (inbox or sent mail) are available for deleted accounts (except those deleted through our Sentinel SAFE project)." (p. 7)	Does not say	• "A preservation creates a snapshot of the information in or about the account at a particular point in time, but there is no update of the information throughout the preservation period." (p. 22) • Free MSN and Hotmail accounts are "typically deleted after 60 days of inactivity. Then if the user does not reactivate their account, the free MSN Hotmail and free Windows Live Hotmail account will become inactive after a period of time." (p. 7) • Microsoft only stores the "e-mails a user has elected to maintain in the account." (p. 8)
Can law enforcement monitor user account without user knowledge?	"If restricting the user's access to the profile will impede an investigation, you can request that private messages be output to flat file for preservation before a subpoena is served." (p.4)	Will lock accounts but keep them viewable upon receiving preservation request. Law enforcement can ask not to lock but then user still has ability to delete and modify (pp. 8, 9)	• Default upon preservation request is that account is still publicly viewable but user will no longer be able to log into account (p. 8) • upon law enforcement request that user not be notified of investigation, MS "will output to a flat file the specific information for which preservation is sought that is available at the time the request is processed." In this situation, user retains access to account, and "interim changes . . . may not be recorded." (p. 8)	• Default upon preservation request is that account is still publicly viewable but user will no longer be able to log into account (p. 8) • upon law enforcement request that user not be notified of investigation, MS "will output to a flat file the specific information for which preservation is sought that is available at the time the request is processed." In this situation, user retains access to account, and "interim changes . . . may not be recorded." (p. 8)	Does not say	Does not say
Does site have exception for emergency disclosure?	"MySpace may disclose private information to law enforcement without a subpoena in limited, emergency situations in which the safety of a MySpace user or member of the public is at risk and there is insufficient time for the law enforcement agency to obtain a subpoena." (p.3)	Does not say	MySpace can disclose info when it "believes in good faith that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay." Must meet "ECPA's threshold requirements." (p.12) • MS has special 24/7 emergency phone hotline (p.12) • Form asks 3 questions: nature of emergency? Whose death/serious physical injury is threatened? What information that MS has is needed? (page 16)	MySpace can disclose info when it "believes in good faith that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay." Must meet "ECPA's threshold requirements." (p.11) • MS has special 24/7 emergency phone hotline (p.11) • Form asks 3 questions: nature of emergency? Whose death/serious physical injury is threatened? What information that MS has is needed? (p. 14)	MSN "will respond to emergency requests outside normal business hours if the emergency involves 'the immediate danger of death or physical injury to an person . . .' as defined in 18 U.S.C. § 2702(c)(4) and (b)(8). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorist threats, etc." (p. 1)	MSN "will respond to emergency requests outside normal business hours if the emergency involves 'the immediate danger of death or physical injury to an person . . .' as defined in 18 U.S.C. § 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorist threats, etc." (p. 3)
Does site charge law enforcement fees?	Does not say	Does not say	Does not say	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	Does not say	Signed fax on law enforcement letterhead with contact info (pp. 8, 13)	Signed fax on letterhead (page 8)	Signed fax or email on letterhead (p. 8)	Does not lay out specific requirements but fax numbers and hotline are listed (p. 1)	Preservation request from law enforcement (p. 22)
Does site address fake accounts created by law enforcement?	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Does not say	Can get user consent (p. 14)	Can get user consent (page 15)	Can get user consent (p. 13)	Does not say	Does not say
How will site deliver data?	Does not say	Delivered in electronic files (spreadsheet) (p. 10)	Delivered in electronic files (9-11)	Delivered via email in Excel spreadsheet (p. 8)	Does not say	Does not say
Other info?	• MS "recommend[s]" that law enforcement agents create an account "to understand the full functionality of the site." (p.1) • approximately a 2-week turnaround for responding to "court-requested information" (p. 4) • User info on site "is not necessarily accurate. Users do not need to confirm their email address, nor provide verified information. Users may also fake IP addresses if they use a proxy." (p.3) • MS terms of service allows MS to "review 'private' content at our discretion." (p. 6)	"MySpace is committed to a high level of cooperation with law enforcement to assist in investigating and identifying those involved in electronic crime and other crime with an electronic component"(p.4)	"MySpace is committed to a high level of cooperation with law enforcement to assist in investigating and identifying those involved in activity that undermines this vision." (p.3)	• Guide potentially contains a quick reference sheet for law enforcement, including a chart showing what legal process MS thinks is required for different types of information. (p. 16) • First time MySpace's Sentinel SAFE project is detailed. The project removes users identified as sex offenders. "The information contained in and related to the profile, including photos, private messages, etc. are preserved by MySpace." (p. 6) MySpace also automatically preserves the data of users who are identified as registerd sex offenders. (p.6) • Guide includes information telling law enforcement agents where to find MySpace information that may reside on a user's computer, such as MySpace Messenger IM client logs, cookie data, cached MySpace pages, and stored login information. (pp. 7-8)		Much of guide is devoted to describing the various online services offered by MSN, such as Windows Live, Xbox Live, MSN, MSN Groups, Windows Live Spaces (p. 4)
Sample forms or sample language?	"The time will come when you need to draft a subpoena in order to request private information" so MS includes info on how to draft subpoenas and court orders (p.4)	Sample Supoena (p.12), Preservation Request Letter (p13), Consent Form (p.14)	Sample subpoena and search warrant language (p.12), Preservation Request Letter (p.14), Consent Form (p.15), Emergency Disclosure Form (p16)	Sample subpoena and search warrant letter (pp. 11-12), preservation request letter (p. 12), consent form (p. 13), emergency disclosure form (p. 14).		

	YAHOO!	AOL	craigslist	ebay PayPal	photobucket
Date	**Updated**	**March 2010**	**Jan 29, 2010**	**Updated**	**Updated**
Date, length, link (if available) and other info	Undated, 17 pages	March 2010, 19 total pages, but were only given 12 (appear to be missing pages 4-6 and 15-18)	Jan. 29, 2010, online document, 1 page, also available at http://www.craigslist.org/about/help/subpoenas_and_search_warrants	Undated, two pages	Undated, eight pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	"ECS for communications including but not limited to email and Messenger" / "RCS for purposes including but not limited to storage of photos and files." • *subpoena* for "basic subscriber information, contents of communications on RCS, contents in electronic storage for over 180 days." • *2703(d) order* for "transactional records (e.g., Messenger or Chat logs, IP address infomration associated with any activity other than log-in), anything obtainable with a subpoena." • *search warrant* for "Contents in electronic storage for 180 days or less, anything obtainable with a sbupoena or 2703(d) order" (p. 11)	Distinguishes between • *subpoena* for "subscriber information," including "name, email addresses, and screen names, addresses, detailed billing records or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned netowrk address, and the means and source of payment for such service (including any credit card or bank account number)." • *2703(d) court order* "is required to compel disclosure of a range of IP connection logs." (p. 12) • *search warrant* for "subscriber information" obtainable under subpoena, "transactional information, including: logs of Internet Protocol ("IP") address connections, including dates, times, and time zones, and any ANI information made available to AOL, address books, buddys lists, and account history, including contacts with AOL support services and records of action taken online by the subscriber or by AOL support staff in connection with the service." • *search warrant* for "all electronic or wire communications (including e-mail text, attachments, and embedded files) in electronic storage by AOL, or held by AOL as a remote computing service, within the meaning of the Stored Communications Act, all photos, files, data, or information in whatever form and by whatever means they have been created or stored, all profiles." (pp 7-9)	Does not say	• signed fax (non-subpoena) "eBay can provide the following information for users under investigation of illegal activity only: contact name, city, state, ZIP, and telephone number, all email addrsses and eBay User ID's added to account with date/time stamps, eBay Fraud complaints (if requested)" • subpoena for "full eBay contact details, including the billing and mailing address, eBay IP addresses: time of registration and at time of item listing, complete listing and/or bid history - 2 year max (including bidder information if specifically requested), credit card and checking acount information added to an eBay account (if available)" • subpoena for all records relating to a PayPal user, including "all PayPal account information including, SSN, names, addresses, phone numbers, email addresses, PayPal IP addresses (at each login), financial instruments added to PayPal account, complete PayPal transactional information (including complaints if requested and available)" (p. 2)	"The types of process necessary to permit Photobucket to produce each category of information under the SCA differs only slightly." • subpoena for "first name, last name, user/screen name, ZIP code, country, email address, account creation date/time" • subpoena for "Date and IP for most recent account access, Registration IP, Banned date/time (if account banned), Date/Time of Upload or Modification of file, Upload IP for files uploaded after June 1, 2007" • court order, search warrant, or subpoena where governent provides prior notice to subscriber for "image and video content in a user's account" (pp. 3-4)
How does site define and/or distinguish different types of user information	Subpoena: basic subscriber information, contents of communications stored as a remote computing service provider, contents in electronic storage over 180 days (p. 11) Court order: Transactional records such as IP logs, messenger or chat logs; search warrant: contents in electronic storage less than 180 days (p. 11)	Subpoena will get "subscriber information:" names, email, physical address, billing records, length of service, phone number, credit card or bank account numbers, IP addresses (pp. 7-8) Search warrant will get "transactional" and "communications" info: IP logs, address books, buddy lists, account history, emails (including attachments), photos or files stored with AOL (p. 9)	Does not say	• No legal service required to access: Contact information, city, state, ZIP code, email addresses, fraud complaints, account listings, and bid history (p. 2) • Subpoena, court order, or warrant to access: billing and mailing address, IP addresses, credit card, checking account information, Social Security numbers	Basic user (subpoena): name, user name, ZIP code, country, email, account creation date (p. 4) IP logs: subpoena, court order, search warrant or user consent (p. 4)
What other info is available?	Can provide files uploaded on Flickr (p. 9)	AOL's Bebo service can only be searched with proper ID. Data retained for past 500 days (p. 19)	Does not say	May be able to get information on accounts linked/related to subject (p.1)	Images and video available by subpoena if subscriber given notice; available with court order or warrant otherwise (p. 4)
How does LE Guide address IP and other logs?	IP logs available with a court order (p. 11)	2703(d) court order required (p. 9)	Does not say	Can be provided (p. 2)	IP logs: subpoena, court order, search warrant or user consent (p. 4)
How long is data generally retained? How long in reponse to preservation request?	"Yahoo! Will preserve information related to a subscriber or customer for 90 dyas, which may be extended for an additional 90 days by a request to extend the preservation." (p. 11)	Sample preservation request asks AOL to preserve data for 90 days. (p.11)	Does not say	eBay keeps most account records indefinitely and transactional records for two years. PayPal keeps all records indefinitely (p. 1)	Data is retained one year; will preserve files requested for 90 days (p. 4)
Is content that has been changed or deleted by user (including private messages) still available?	"Yahoo! will be unable to search for and produce deleted material, including email and Group posts, unless such request is received within 24 hours of the deletion and is specifically requestsed by prior legal process. In most cases where deleted content is requested, Yahoo! will seek reimbursement for any engineer time incurred in connection with the request." (p. 7)	Does not say whether deleted email can be recovered	Does not say	Does not say	Active users can delete files from account (p. 4)
Can law enforcement monitor user account without user knowledge?	Does not say	Does not say	Does not say	Does not disclose law enforcement inquiries to account holders (p. 1)	Does not say
Does site have exception for emergency disclosure?	"Yahoo! Is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records [. . .] if Yahoo! believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay." (p. 12) • Emergency disclosure request has set of seven questions: Nature of emergency? Who is threatened? What is nature of threat? Why would normal disclosure be insufficient? What info is needed? Explain how info will avert threat? Attach any electronic evidence of threat? (p. 16)	"The Stored Communications Act permits an Internet service provider to disclose the content of electronic or wire communications or customer records to law enforcement 'if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure withouot delay of communications [or records] relating to the emergency.'" "In the event of an emergency, please telephone AOL's Public Safety and Criminal Investigations unit at [redacted] and provide us with specific facts concerning the emergency that you believe requires immediate disclosure of communications or records relating to the emergency." The specific facts should include: description of the emergency, explanation that the danger is imminent, what specific records are needed (p. 13)	Does not say	Has a "First Responder" service that can return calls within 24 hours and process complaints quickly (pp. 1-2)	"Photobucket will also exercise its discretion under the SCA to release information without legal process where an imminent threat of death or serious physical injury to a person exists that necessitates disclosure" Asked to provide information on the nature of the emergency, the name of the person who is threatened, the specific information in Photobucket's possession related to the emergency. (p. 5)
Does site charge law enforcement fees?	Federal law "requires law enforcement to reimburse providers like Yahoo! for costs incurred responding to subpoena requests, court orders, or search warrants." Lists a fee schedule: • Basic subscriber records: "approx. $20 for the first ID, $10 per ID thereafter" • Basic Group Information (including information about moderators): "approx $20 for a group with a single moderator" • Contents of subscriber accounts, including email: "approx. $30-$40 per user" • Contents of Groups: "approx. $40-$80 per group" (p. 12) • Also, where deleted content is requested, Yahoo! will seek reimbursement for any engineer time incurred in connection with the request." (p. 7)	Does not say	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	Sent by fax (p. 11)	Signed fax on department letterhead with law enforcement ID (pp. 11-12)	"Official requests for release of records can be submitted by email, fax, or mail."	Signed fax on department letterhead for user contact info, subpoena, court order, or search warrant requierd for full records (p. 2)	Correspondence must include contact information where files will be sent (p. 6)
Does site address fake accounts created by law enforcement?	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Can get user consent (p. 13)	Will release data upon user consent through form (p. 14)	Does not say	Does not say	Can get user consent (p. 4)
How will site deliver data?	Unclear how Yahoo! delivers information	mail (p. 8)	Can respond via fax, email, or mail	Provides records electronically, via secure website, or CD via Fed Ex (p. 1)	Delivered via CD (p. 6)
Other info?		Contains a search warrant directory page, listing fax numbers for fed and military warrants, state or local agencies, and particular jurisdictions, including California, Florida, Minnesota, Washington (state), New York (p. 10) The site also has a three paragraph description of BEBO searches and the information it can provide to LE (p. 19)	The guide is a page from Craigslist's website: http://www.craigslist.org/about/help/subpoenas_and_search_warrants	• Law enforcement must provide a minimum of name, email address and User Name (for eBay investigations) to locate the correct account. (p. 1) • Turnaround time for requests is typically 10-15 business days (p. 2) • but Ebay/PayPal make" listing and member information immediately available to law enforcement via Leadsonline's First Responder Service." (p. 1)	• The guide lays out how it reports accounts containing child pornography, using NCMEC Reporting. (p. 5) • The guide contains an FAQ for law enforcement along with information on how the data it sends to LE is formatted (pp. 6-7) • This guide has what appears to be the same reference sheet obtained in either the 2005 or 2007 MySpace guide (p. 8)
Sample forms or sample language?	Yahoo! provides sample preservation request letter (p. 14), sample language for subpoenas, court orders, and search warrants (p. 15), emergency disclosure request (p. 16), and sample consent form (p. 17)	Sample subpoena language and subpoena format requirements (pp. 7-8), sample search warrant (p. 9), sample preservation request (pp. 11-12), emergency voluntary disclosure request (p. 13), user consent form (p. 14)			Language for preservation and emergency requests (pp. 4-5)

	myYearbook	NING	STICKAM	TAGGED	IMVU
Date	**April 2010**	**July 2009**	**April 26, 2010**	**Updated**	**Updated**
Date, length, link (if available) and other info	April 2010, four pages	July 2009, four pages	April 26, 2010, 16 pages	Undated, 16 pages	Undated, 2 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	• No legal process required for "Public Information," such as profile page, profile images. • *subpoena* for "General Information," including user name, user ID, DOB, age, location (if known), school (if known), email address, password, date joined, user name changes, DOB changes, violations of terms of service, IP logs of last 6 months (login times only), IP addresses, date and time logged in, all profile pictures in account (though accounts deleted by MYB or the user willnot have any images available) • *search warrant* for "Communications/private Information," including private messagees, instant messages, embedded images in messages. (pp. 1-2)	"Ning can provide you with the following information once we receive a subpoena, search warrant or court order" • *subpoena* for the registration email of the Network Creator and Members who uploaded the content, registration IP addresses, Usernames, credit card information (if any) • *search warrant* for all images and videos of suspected child pornography, date/time stamped IP addresses at time member uploaded content in question, any and all messages received from creators and members, subject line and date/time stamp of all automated email notifications (pp. 2-3)	Non-public information requires legal process in compliance with ECPA	"To request private (non-public) information from Tagged about a specific profile or user, we requires a subpoena, search warrant or other legal process. The following list is private content that is not publicly accessible" • "IP logs (recorded at time of login), Date profile created, Dates and times of login (PST), E-mail address provided by user, ZIP code provided by user, Name provided by user, Screen Name, Private Messages" • "The following are only retained if the user has not deleted them from their page: Confessions, Boxxes, Journals." (p. 6)	• *subpoena* for "basic account information" will include "avatar name, e-mail address, customer ID (all unique) as well as the IP address used to register the account and any device fingerprints on file [. . .] If account communications are requested, IMVU will provide the text of web-based messages and a summary of realt-time chats (via IMVU's 3D client) that will include the accounts participating in chats but not the actual text of the chat" (page 1)
How does site define and/or distinguish different types of user information	Public info available without legal process: Profile page, profile images; General info (subpoena): user name, ID, birthday, age, location password, date joined, changes to profile, IP logs, profile pictures (pp. 1-2) Communications (search warrant): private messages, instant messages, any images embedded in messages (p. 2)	Subpoena: email, IP address, username, credit card information (if available) (pp. 2-3) Search warrant: Images, videos, IP address, all messages (p. 3)	Subpoena required for basic user information, log in information, and stored files (p. 4) Court order required for full access to profile; search warrant required for private user messages (p. 4)	Subpoena: IP logs, date profile created, dates of login, email address, ZIP code, name, screen name (p. 6) Unclear what level of legal process is required for messages (p. 6)	Basic account information (subpoena): avatar name, email address, customer ID, IP addresses and device fingerprint (p. 1) Unclear what legal process is required for text of web messages and chat logs (p. 1)
What other info is available?	Does not say	Images available with search warrant (p. 3)	Video, audio, and photo files available via subpoena (p. 2)	Not clear what level of legal process is required for this information	Does not say
How does LE Guide address IP and other logs?	Can be produced with subpoena (p. 2)	IP addresses can be produced (p. 3)	IP logs available with subpoeana (p. 1, 4)	IP logs are available with subpoena (p. 6)	Does not say
How long is data generally retained? How long in reponse to preservation request?	Active accounts kept indefinitely, IP logs retained for 6 months (p. 3)	90 days unless preservation request has been made (pp. 1-2)	Most data retained 90 days but will be retained longer if given a preservation request (p. 3)	"Tagged retains information on its users for certain periods of time. [...] To the extent information that was scheduled to be deleted needs to be retained by Tagged due to an on-going law enforcement investigation, Tagged will do so in response to a written law enforcement preseration request." • IP logs "are saved for 6 months" • Private messages "are retained until the user removes them. Tagged may be able to recover them if the sender's Tagged User ID or email address is provided." • Sent Mail "is only retained if the user saves their outgoing messages." • Trash Mail "(mail that has been read and discarded) is retained 30 days or less." • Deleted Accounts "mail is available for deleted accounts with the same rules as active accounts." (pp. 7-8)	"IMVU does not have a policy for the regular purging or removal of account records but communication data may be missing or incomplete after 6 months." (p. 1)
Is content that has been changed or deleted by user (including private messages) still available?	• Describes that "accounts which have been deleted by either MYB staff or the user will not have any images available." (p. 3) • "Accounts which have been deleted by MYB staff or deleted by the user cannot be seen on the site. Like active accounts, all information is still available except for profile pictures." (p. 3) • Does not say regarding private messages. • Regarding instant messages "No general records are kept on instant messages. If a member is reporting a violation of TOS, the conversation is saved and provided to MYB. Those IM conversations are retained."	Does not say	• Active users can modify and delete account infomration and files (p. 3) • Does not say whether there is a different retention schedule for email messages	• Users can delete or modify information (p. 7) • Mail is retained until user deletes the messages, though undeleted mail can be accessed after users delete accounts with Tagged (p. 7)	Does not say
Can law enforcement monitor user account without user knowledge?	Does not say	On discovery of illegal activity, account is disabled and member is informed that law enforcement have been contacted (p. 2)	Does not say	Once preservation request is received "the account will still be publicly viewable, the user will not be able to log into his/her account, information in the Sent Mail/Trash folder is still subject to automatic deletion." "If restricting the user's access to the profile will impede and investigation, you may request that private messages be output to a flate file for preservation before a subpoena is served.You must specifically request in the letter that the user not be notified of the investigation if you do not want the subject account to be locked." (p. 8)	"In the legal documentation please be specific if the account should remain enabled. If IMVU becomes aware of an account with suspicious or illegal activity it will likely be disabled. If leaving an account enabled will assist in an investigation, please make sure this is stated when submitting the subpoena, search warrant, or other court-ordered demand." (p. 2)
Does site have exception for emergency disclosure?	Does not say	Does not say	Can release when it "believes in good faith that an emergency involving danger of death or serious physical injury" (p. 4)	Does not say	Does not say
Does site charge law enforcement fees?	Does not say	Does not say	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	Faxed requests (p. 1)	Requests involving legal process must be sent via fax and certified mail (p. 1)	Correspondence must identify officer and information sought (pp. 4-5)	Faxed letter on department letterhead (pp. 6, 13)	When requesting account data, subpoena or search warrant are required (p. 2)
Does site address fake accounts created by law enforcement?	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Will accept user consent (page 3)	Does not say	Does not say	Can get user consent (p. 14)	Does not say
How will site deliver data?	Does not say	Can send via mail (p. 2)	Delivered via email (p. 5)	Looks like it is delivered electronically (pp. 10-11)	Does not say
Other info?	MYB takes a snap shot of the site every night and is kept on a backup file for 7 days. After 7 days, the file is deleted. MYB also keeps the file taken on the last calendar day of the month for two months before deleting it. (p. 4)	Ning's guide is particularly directed toward the discovery of child pornography, outlining NCMEC Reporting requirements, as well as outlining ways international jurisdictions can use ECPA to get information (p. 3) Ning also says that if LE wants child pornography mailed to it, it must directly mandate so in the search warrant, as Ning does not want to be prosecuted for transmission of child pornography (p. 2)		Guide contains a page devoted to "Understanding IP Addresses" (p. 15) and a page with "Websites and Resources" for LE (p. 16)	• Disclaimer that IMVU does not verify customer data (p. 1) • If request is related to ID theft, victims can request information without a subpoena or warrant (page 2)
Sample forms or sample language?				sample subpoena (p. 12), sample preservation request letter (p. 13), sample consent form (p. 14)	Guide instructs that "When requesting account data, please have the subpoena or search warrant request: 'Account data for the account(s) matching the Avatar name, e-mail or IP addresses *[insert known data here]* and for any account(s) that appears to be controlled by the same person." (p. 2)

ELECTRONIC FRONTIER FOUNDATION

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	twitter	facebook	facebook	facebook	myspace a place for friends	myspace.com
Date	**Undated**	**2008**	**2009**	**2010**	**2005**	**March 2006**
Date, length, link (if available) and other info	Available on Twitter site at: http://support.twitter.com/entries/41949-guidelines-for-law-enforcement	February 2008, five pages	2009, 11 pages	May 2010, 5 pages	September 2, 2005, 7 pages	March 13, 2006, 16 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	Addresses but does not distinguish: "We require a subpoena, court order, or other valid legal process to disclose information about our users." By default, most Twitter profile information is public. This includes, according to the privacy policy, name and username. It also may include a short bio, cell phone number, location, address book, a picture, "the messages you Tweet and the metadata provided with Tweets, such as when you Tweeted, but also the lists you create, the people you follow, the Tweets you mark as favorites or Retweet and many other bits of information." "Non-public information about Twitter users is not released unless we have received a subpoena, court order, or other valid legal process document."	Does not say	• Subpoena for non-content (basic subscriber info), • ECPA 2703(d) order for limited content (e.g. messages over 180 days), • search warrant for remaining content (p. 3)	"we will provide records as required by law." (p.2)	• Most profile information is publicly viewable and available. Publicly available information includes journal entries (in most cases), images, user comments, and public profile information." (p.2) • MS requires a subpoena for following info: -IP logs (recorded at time of login), Dates and times of login (PST), Email address, ZIP code, name, private messages (pp.2-3)	"Most profile information is publicly viewable and available." (Guide includes instructions for law enforcement to download this info) • Non-public information requires subpoena, search warrant, or other legal process • Non-public info includes: IP logs (recorded at time of login), Date profile created, Dates and times of login, E-mail address, ZIP code, Name, Private Messages, Private blogs (some info may not be accurate) (p. 6) • Information provided in response to subpoena: email address, IP Logs, private messages (p.10)
How does site define and/or distinguish different types of user information	Law Enforcement Guide, TOS & Privacy Policy only distinguish between public and non-public information	Does not distinguish between basic subscriber information and other information (p. 4)	User ID number, email address, time account was created, most recent logins, registered mobile number, whether account is publicly viewable (p. 6) "User Neoprint": Contact information, mini-feed, status update history, shares, notes, wall posts, friend listings (including their IDs), group listings (including group member IDs), future and past events, video listings (p. 6)	User ID number, email address, date/time account was created, most recent logins, registered mobile number (p. 4) "Expanded Subscriber Content (sometimes referred to as Neoprint)": Contact information, mini-feed, status update history, shares, notes, wall postings, friend listings (include friend IDs), group listings (including group member IDs), future and past events, video listings (p. 4)	Guide only distinguishes between public and non-public information (p.2)	Guide only distinguishes between public and non-public information (p. 6)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	twitter	facebook	facebook	facebook	myspace a place for friends	myspace.com
What other info is available?	Twitter does not host any content other than tweets. This includes any video or images that users may share through their accounts.	User photos, group contact information (p. 4)	"User Photoprint": User uploaded photos and photos tagged with user's name, group contact information, private messages (p. 7)	"User photos (sometimes referred to as User Photoprint)": User uploaded photos and photos tagged with user's name, group information, private messages (p. 4)	unclear	Unclear whether photos and other content are released (p. 6)
How does LE Guide address IP and other logs?	Twitter's servers automatically record information ("Log Data"), which may include information such as IP address, browser type, the referring domain, pages visited, and search terms. Other actions, such as interactions with advertisements, may also be included in Log Data.	• Logs are available and include: Script - script executed, Scriptget - additional information passed to the script, Userid - Facebook user id of the account active for the request, View time - date of execution in Pacific Time, IP - source address	• now have a limited capacity of retrieving specific logs and are technically limited in providing "everything" within a requested date range. We are unable to testify to the completeness of the data. • Logs include same data as 2008 • IP logs contain content and are treated as such under ECPA (p. 7)	• IP logs contain same data as 2008/09 and also include Session Cookie -- HTTP cookie set by user session • Logs are often incomplete, but if available will be provided (p. 4)	IP Logs are available for up to ninety days after a user's last login.(p.3)	Available through subpoena. Info includes time and date stamp (p. 10)
How long is data generally retained? How long in reponse to preservation request?	"Twitter retains different types of information for different time periods. Given Twitter's real-time nature, some information may only be stored for a very brief period of time."	90 days (page 3), though IP data may be retained shorter or longer depending (p. 5)	90 days, but an extension can be made if necessary (p. 6)	90 days, but an extension can be made if necessary. "By default we will return data no older than 90 days prior to the date we receive the request." (p. 2)	• IP Logs are available for up to ninety days after a user's last login. • Private Messages in an active account User's Inbox - Retained until user removes them. • Sent Mail - Retained for 14 days. • Trash Mail - Retained 30 days or less. Users can empty their trash at any time. • Deleted Accounts - No mail is available for deleted accounts. • User ID, IP Address, Login date stamps are retained for up to 90 days after account • Profile information is available for up to ten days after account deletion.(p. 3)	• "MySpace does not retain information that is altered on or removed from an active profile. Once a change is made, existing information is overwritten." (p.7) • MySapce has different retention times for different types of info but law enforcement can request preservation for longer (p. 8) • Messages retained as long as not deleted; sent mail retained for 14 days; trash mail retained 30 days or less unless user empties trash, which permanently deletes message (p. 7)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	twitter	facebook	facebook	facebook	myspace a place for friends	myspace .com
Is content that has been changed or deleted by user (including private messages) still available?	unclear	Content available as long as not deleted by user (page 4)	• If user has saved messages, they can be recovered. If deleted by user, they cannot be recovered (page 7) • If a profile is changed or updated, deleted content is not retained (page 6)	If messages are retained by user, they are available (page 4)	• MS cannot recover deleted messages unless it is in another user's Sent Mail; • "MySpace.com does not retain information that is altered/ removed on an active profile. Once a change is made, existing information is overwritten." (p.3)	• Myspace doesn't retain altered or removed info. However, MySpace may be able to retreive deleted messages from another user who sent or received email. User ID, IP Address, Login date stamps are retained for up to 90 days after account deletion. Profile information is available for up to ten days after account deletion. (p. 7)
Can law enforcement monitor user account without user knowledge?	"Twitter's policy is to notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order."	Does not say	Will normally disable account unless law enforcement clearly specify that doing so will hurt investigation (page 5)	Will normally disable account unless law enforcement clearly specify that doing so will hurt investigation (page 2)	"If restricting the user's access to the profile will impede an investigation, you can request that private messages be output to flat file for preservation before a subpoena is served." (p.4)	Will lock accounts but keep them viewable upon receiving preservation request. Law enforcement can ask not to lock but then user still has ability to delete and modify (pp. 8, 9)
Does site have exception for emergency disclosure?	Does not say.	Does not say	Can provide upon answering 3 questions: Describe emergency? Provide ID of users involved? Provide location of evidence? (pp. 8, 10)	Can provide upon answering 3 questions:Describe emergency? Provide ID of users involved? Provide location of evidence? (p. 5)	"MySpace may disclose private information to law enforcement without a subpoena in limited, emergency situations in which the safety of a MySpace user or member of the public is at risk and there is insufficient time for the law enforcement agency to obtain a subpoena." (p.3)	Does not say

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	twitter	facebook	facebook	facebook	myspace a place for friends	myspace .com
Does site charge law enforcement fees?	Does not say.	Reserves right to charge reasonable fees (p. 2)	Reserves the right to charge reasonable fees (p. 5)	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	"Preservation requests must be signed, include a valid return email address, and sent on law enforcement letterhead."	Request to preserve that includes law enforcement officer ID, contact informtion, name of agency (p. 3)	Request to preserve from law enforcement with ID, name of agency, and contact info (p. 5)	Request to preserve from law enforcement, with ID, name of agency, and contact info (p. 3)	Does not say	Signed fax on law enforcement letterhead with contact info (pp. 8, 13)
Does site address fake accounts created by law enforcement?	Not addressed specifically, but Twitter acknowleges that users may create fake or anonymous profiles However, Twitter's "Rules" prohibit impersonation: "You may not impersonate others through the Twitter service in a manner that does or is intended to mislead, confuse, or deceive others"	Will disable accounts that violate terms of service, including fake police accounts (p. 2)	Will disable fake police accounts (p. 3)	Will "always disable accounts that supply false or misleading profile information or attempt to technically or socially circumvent site privacy measures." (p. 2)	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Yes - Twitter may "share or disclose your information with your consent, such as when you use a third party web client to access your Twitter account"	Does not say	Will release data upon user consenting through form (pp. 8, 11)	Does not say	Does not say	Can get user consent (p. 14)
How will site deliver data?	Does not say.	Generally through email (p. 3)	Generally through email (p. 5)	Does not say	Does not say	Delivered in electronic files (spreadsheet) (p. 10)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	twitter	facebook	facebook	facebook	myspace a place for friends	myspace .com
Other info?	N/A	Facebook may be able to retrieve specific information not described in guide (p. 5)	"Special Requests": Facebook may be able to retrieve specific information not described in guide (p. 9)	"We are required to disable accounts engaged in illegal activity, even if that activity is brought to our attention through a request for records." (p.5)	• MS "recommend[s]" that law enforcement agents create an account "to understand the full functionality of the site." (p.1) • approximately a 2-week turnaround for responding to "court-requested information" (p. 4) • User info on site "is not necessarily accurate. Users do not need to confirm their email address, nor provide verified information. Users may also fake IP addresses if they use a proxy." (p.3) • MS terms of service allows MS to "review 'private' content at our discretion." (p. 6)	"MySpace is committed to a high level of cooperation with law enforcement to assist in investigating and identifying those involved in electronic crime and other crime with an electronic component"(p.4)
Sample forms or sample language?	N/A	N/A	Emergency Disclosure Form, User Consent to Release Form	Emergency Disclosure Form	"The time will come when you need to draft a subpoena in order to request private information" so MS includes info on how to draft subpoenas and court orders (p.4)	Sample Supoena (p.12), Preservation Request Letter (p13), Consent Form (p.14)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	myspace.com	myspace.com	msn	msn
Date	**June 2006**	**2007**	**2006**	**2008**
Date, length, link (if available) and other info	June 23, 2006, 16 pages	November 1, 2007, 15 pages	July 2006, 2 pages	March 2008, 22 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	MySpace is both an ECS and RCS (p.4) • *subpoena* for "basic user identity, log-in information, and stored files", • *§ 2703(d) court order* for "user's date of birth, gender, hometown, and occupation, as well as historical private message header information." • *search warrant* for private user communications less than 180 days old. • *Subpoena or court order with prior notice to the subscriber (or delayed notice under 18 U.S.C. § 2705)* for Stored user files (photos, videos, blogs, classifieds, messages posted on forums or groups, address book and calendar contents) • *pen register/trap and trace order* for ongoing information about user's IP address each time they log-in to their account (pp. 4-7) • Law enforcement can obtain publicly available info without MySpace's assistance. (p. 4,5)	"Depending on the type of information sought, ECPA may require the use of a different form of legal process, and the period MySpace retains the information may differ." (p. 4) • subpoena or § 2703(c)(2) demand for "Basic user identity information," including "date profile created; first and last name provided by user; user ID; e-mail address provided by user; ZIP code, city, and country provided by user; account creation date and time; and the IP address at the time of sign-up." • subpoena or § 2703(c)(2) demand for historical "logs showing the IP address assigned to the user and the date stamp at the time the user accessed his or her profile." • Pen register/trap and trace order to "caputre log-in IPs prospectively." • Search warrant for messages less than 180 days old. • Subpoena or court order (or delayed notice under 18 U.S.C. § 2705) for messages over 180 days old. • Subpoena, civil investigative demand, or court order for "profile information including photos, videos, blogs, blog comments by other users, the identities fo the friends and 'About Me' entries." • § 2703(d) court order for "user's date of birth, gender, hometown, and occupation, as well as historical private message header information, excluding subject."(pp. 5-6)	ECPA "governs what legal documentation is required in order for Microsoft's Online Service records custodian to disclose customer account information and email content." • *subpoena* for basic subscriber information, including "name address, length of service (start date), screen names, other email accounts, IP address/IP logs/Usage logs, billing information, and e-mail content greater than 180 days old as long as the governmental entity follows the customer notification provisions in ECPA (see 18 U.S.C. § 2705)." (p. 2) • *2703(d) order* "will compel disclosure of all of the Basic Subscriber information available under a sbupoena plus the Address Book, Buddy Lists, the rest of a customer's profile not already listed above, internet usage logs (WEBTV), e-mail header information (to/from) excluding subject line, and e-mail content greater than 180 days old as long as the governmental entity follow the customer notifications provisions of ECPA (see 18 U.S.C. § 2705)." (p. 2) • *search warrant* is required for all email content under 180 days. (p. 2)	ECPA "sets forth the appropriate legal process required to compel Microsoft's Online Service Records Custodians to disclose customer records and contents" • *subpoena* for basic subscriber information, including "name, address, length of service (start date), screen names, other email acounts, IP address/IP logs/Usage logs, billing information content (other than e-mail, such as Windows Live Spaces and MSN Groups) and e-mail content more than 180 days old as long as the governmental entity follows the customer notification provisions in ECPA (see 18 U.S.C. §§ 2703(b), 2705) • *2703(d) order* "will compel disclosure of all of the basic subscriber information available under a subpoena pluse the e-mail address book, Messenger contact lists, the rest of a customer's profile not alread listed above, internet usage logs (e.g. WEBTV or MSN Internet Access), and e-mail header information (to/from) excluding subject line." • *Search warrant* "will compel disclosure of all information available with a court order issued pursuant to 2703(d) (as listed above), plus all contents (if prior notice is not provided or an order for delayed notice is not obtained), and is the only means to compel the disclosure of e-mails, including subject line, in electronic storage 180 days or less."(p. 22) • "as Microsoft receives and processes legal process for its online services in the Ninth Circuit, [pursuant to *Theofel et al v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003)]Microsoft discloses both opened and unopened e-mail in electronic storage for 181 days or less only upon pursuant to a search warrant.
How does site define and/or distinguish different types of user information	basic "user" ID info including user's name, email address, ZIP code, city & country, account creation date/time, IP address at time of signup -- all available via subpoena (pp. 6-7) user's birthday, gender, hometown, occupation, private message header information; search warrant: messages less than 180 days old -- all available via court order: (p. 6)	Basic user ID (subpoena): date profile created, name, user ID, email address, ZIP code, city, county, account creation date, IP address; other (court order) IP logs, birthday (pp. 5-6) Search warrant: private messages less than 180 days old (p. 5)	Basic (subpoena): name, address, length of service, screen names, IP address, IP logs, billing info, email greater than 180 days (p. 2) Full profile (court order): address book, buddy list, email header info, email content great than 180 days; Email (warrant): all messages less than 180 days old (p. 2)	Basic (subpoena): name, address, length of service, screen names, IP address, IP logs, billing info, email greater than 180 days (p. 22) Full profile (court order): address book, buddy list, email header info, email content great than 180 days; Email (warrant): all messages less than 180 days old (p. 22)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	myspace.com	myspace.com	msn	msn
What other info is available?	Photos, videos, blogs, classifieds can be disclosed with a subpoena (pages 6-7)	Photos, videos, blogs available with subpoena or court order (p. 6)	MSN groups and spaces are considered public, and will be disclosed with subpoena (p. 2)	Can get this information from all of MSN services, such as Xbox Live, Windows Live, etc. (p. 4)
How does LE Guide address IP and other logs?	Can be produced with subpoena (p. 6) Info includes IP address, date and time of log-in at time user accesses profile. Historic IP logs are available, and MySpace can capture IP logs prospectively with Pen/Trap order.	Can be produced with court order (p. 5)	Can be produced with subpoena (p. 2)	Can be produced with subpoena (p. 22)
How long is data generally retained? How long in reponse to preservation request?	• Messages retained as long as not deleted; sent mail retained for 14 days; trash mail retained 30 days or less unless user empties trash, which permanently deletes message (page 7) • Law enforcement can request preservation for longer (p.7) • Pursuant to preservation request: 90 days but can be extended an extra 90 (p. 8)	• Messages retained as long as not deleted; sent mail retained for 14 days; trash mail retained 30 days or less unless user empties trash, which permanently deletes message (page 7) • "MySpace honors all law enforcement preservation requests made during the period the data is available. MySpace also automatically preserves the data of users who are identified as registerd sex offenders and removed from the MySpace site pursuant to MySpace's Sentinel SAFE Project." (p.6) • Pursuant to preservation request: "MySpace will preserve the specific information identified in the request for up to 180 days and will extend the preservation as necessary at your request." (p. 8)	90 days from date of request, but can preserve for up to 270 days (p. 2)	90 days from date of request, but can preserve for up to 270 days (p. 22)

	myspace.com	myspace.com	msn	msn
Is content that has been changed or deleted by user (including private messages) still available?	User can delete and modify account (p.8) If user deletes account: • "User identity and date in the user profile is generally available for up to 10 days after account deletion. Other stored files, such as photos, may be lost at the time of account deletion." • "User ID, IP Address and Login date stamps are retained for up to 90 days after account deletion. • no mail is available for deleted accounts (p.8)	User can delete and modify (p. 6) • "Upon receipt of a preservation request, however, MySpace will capture all user data available at that time, and future actions by the user will not affect the preserved data."(p. 6) • "User identity information is available for one year after account deletion. Other stored files, such as photos, may be lost at the time of account deletion." • "MySpace retains Friend ID, IP Address and Login time and date stamps dating back one year." • "No private messages (inbox or sent mail) are available for deleted accounts (except those deleted through our Sentinel SAFE project)." (p. 7)	Does not say	• "A preservation creates a snapshot of the information in or about the account at a particular point in time, but there is no update of the information throughout the preservation period." (p. 22) • Free MSN and Hotmail accounts are "typically deleted after 60 days of inactivity. Then if the user does not reactivate their account, the free MSN Hotmail and free Windows Live Hotmail account will become inactive after a period of time." (p. 7) • Microsoft only stores the "e-mails a user has elected to maintain in the account." (p. 8)
Can law enforcement monitor user account without user knowledge?	• Default upon preservation request is that account is still publicly viewable but user will no longer be able to log into account (p. 8) • upon law enforcement request that user not be notified of investigation, MS "will output to a flat file the specific information for which preservation is sought that is available at the time the request is processed." In this situation, user retains access to account, and "interim changes . . . may not be recorded." (p. 8)	• Default upon preservation request is that account is still publicly viewable but user will no longer be able to log into account (p. 8) • upon law enforcement request that user not be notified of investigation, MS "will output to a flat file the specific information for which preservation is sought that is available at the time the request is processed." In this situation, user retains access to account, and "interim changes . . . may not be recorded." (p. 8)	Does not say	Does not say
Does site have exception for emergency disclosure?	MySpace can disclose info when it "believes in good faith that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay." Must meet "ECPA's threshold requirements." (p.12) • MS has special 24/7 emergency phone hotline (p.12) • Form asks 3 questions: nature of emergency? Whose death/serious physical injury is threatened? What information that MS has is needed? (page 16)	MySpace can disclose info when it "believes in good faith that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay." Must meet "ECPA's threshold requirements." (p.11) • MS has special 24/7 emergency phone hotline (p.11) • Form asks 3 questions: nature of emergency? Whose death/serious physical injury is threatened? What information that MS has is needed? (p. 14)	MSN "will respond to emergency requests outside normal business hours if the emergency involves 'the immediate danger of death or physical injury to an person . . .' as defined in 18 U.S.C. § 2702(c)(4) and (b)(8). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorist threats, etc." (p. 1)	MSN "will respond to emergency requests outside normal business hours if the emergency involves 'the immediate danger of death or physical injury to an person . . .' as defined in 18 U.S.C. § 2702(b)(8) and (c)(4). Emergencies are limited to situations like kidnapping, murder threats, bomb threats, terrorist threats, etc." (p. 3)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	myspace.com	myspace.com	msn	msn
Does site charge law enforcement fees?	Does not say	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	Signed fax on letterhead (page 8)	Signed fax or email on letterhead (p. 8)	Does not lay out specific requirements but fax numbers and hotline are listed. (p. 1)	Preservation request from law enforcement (p. 22)
Does site address fake accounts created by law enforcement?	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Can get user consent (page 15)	Can get user consent (p. 13)	Does not say	Does not say
How will site deliver data?	Delivered in electronic files (9-11)	Delivered via email in Excel spreadsheet (p. 8)	Does not say	Does not say

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	myspace.com	myspace.com	msn	msn
Other info?	"MySpace is committed to a high level of cooperation with law enforcement to assist in investigating and identifying those involved in activity that undermines this vision." (p.3)	• Guide potentially contains a quick reference sheet for law enforcement, including a chart showing what legal process MS thinks is required for different types of information. (p. 16) • First time MySpace's Sentinel SAFE project is detailed. The project removes users identified as sex offenders. "The information contained in and related to the profile, including photos, private messages, etc. are preserved by MySpace." (p. 6) MySpace also automatically preserves the data of users who are identified as registerd sex offenders. (p.6) • Guide includes information telling law enforcement agents where to find MySpace information that may reside on a user's computer, such as MySpace Messenger IM client logs, cookie data, cached MySpace pages, and stored login information. (pp. 7-8)		Much of guide is devoted to describing the various online services offered by MSN, such as Windows Live, Xbox Live, MSN, MSN Groups, Windows Live Spaces (p. 4)
Sample forms or sample language?	Sample subpoena and search warrant language (p.12), Preservation Request Letter (p.14), Consent Form (p.15), Emergency Disclosure Form (p16)	Sample subpoena and search warrant letter (pp. 11-12), preservation request letter (p. 12), consent form (p. 13), emergency disclosure form (p. 14).		

	YAHOO!	AOL	craigslist	eBay PayPal
Date	**Undated**	**March 2010**	**Jan 29, 2010**	**Undated**
Date, length, link (if available) and other info	Undated, 17 pages	March 2010, 19 total pages, but were only given 12 (appear to be missing pages 4-6 and 15-18)	Jan. 29, 2010, online document, 1 page, also available at http://www.craigslist.org/about/help/subpoenas_and_search_warrants	Undated, two pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	"ECS for communications including but not limited to email and Messenger" / "RCS for purposes including but not limited to storage of photos and files." • *subpoena* for "basic subscriber information, contents of communications on RCS, contents in electronic storage for over 180 days." • *2703(d) order* for "transactional records (e.g., Messenger or Chat logs, IP address infomration associated with any activity other than log-in), anything obtainable with a subpoena." • *search warrant* for "Contents in electronic storage for 180 days or less, anything obtainable with a sbupoena or 2703(d) order" (p. 11)	Distinguishes between • *subpoena* for "subscriber information," including "name, email addresses, and screen names, addresses, detailed billing records or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned netowrk address, and the means and source of payment for such service (including any credit card or bank account number)." • *2703(d) court order* "is required to compel disclosure of a range of IP connection logs." (p. 12) • *search warrant* for "subscriber information" obtainable under subpoena, "transactional information, including: logs of Internet Protocol ("IP") address connections, including dates, times, and time zones, and any ANI information made available to AOL, address books, buddys lists, and account history, including contacts with AOL support services and records of action taken online by the subscriber or by AOL support staff in connection with the service." • *search warrant* for "all electronic or wire communications (including e-mail text, attachments, and embedded files) in electronic storage by AOL, or held by AOL as a remote computing service, within the meaning of the Stored Communications Act, all photos, files, data, or information in whatever form and by whatever means they have been created or stored, all profiles." (pp 7-9)	Does not say	• signed fax (non-subpoena) "eBay can provide the following information for users under investigation of illegal activity only: contact name, city, state, ZIP, and telephone number, all email addrsses and eBay User ID's added to account with date/time stamps, eBay Fraud complaints (if requested)" • subpoena for "full eBay contact details, including the billing and mailing address, eBay IP addresses: time of registration and at time of item listing, complete listing and/or bid history - 2 year max (including bidder information if specifically requested), credit card and checking acount information added to an eBay account (if available)" • subpoena for all records relating to a PayPal user, including "all PayPal account information including, SSN, names, addresses, phone numbers, email addresses, PayPal IP addresses (at each login), financial instruments added to PayPal account, complete PayPal transactional information (including complaints if requested and available)" (p. 2)
How does site define and/or distinguish different types of user information	Subpoena: basic subscriber information, contents of communications stored as a remote computing service provider, contents in electronic storage over 180 days (p. 11) Court order: Transactional records such as IP logs, messenger or chat logs; search warrant: contents in electronic storage less than 180 days (p. 11)	Subpoena will get "subscriber information:" names, email, physical address, billing records, length of service, phone number, credit card or bank account numbers, IP addresses (pp. 7-8) Search warrant will get "transactional" and "communications" info: IP logs, address books, buddy lists, account history, emails (including attachments), photos or files stored with AOL (p. 9)	Does not say	• No legal service required to access: Contact information, city, state, ZIP code, email addresses, fraud complaints, account listings, and bid history (p. 2) • Subpoena, court order, or warrant to access: billing and mailing address, IP addresses, credit card, checking account information, Social Security numbers

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	YAHOO!	AOL	craigslist	eBay PayPal
What other info is available?	Can provide files uploaded on Flickr (p. 9)	AOL's Bebo service can only be searched with proper ID. Data retained for past 500 days (p. 19)	Does not say	May be able to get information on accounts linked/related to subject (p.1)
How does LE Guide address IP and other logs?	IP logs available with a court order (p. 11)	2703(d) court order required (p. 9)	Does not say	Can be provided (p. 2)
How long is data generally retained? How long in reponse to preservation request?	"Yahoo! Will preserve information related to a subscriber or customer for 90 dyas, which may be extended for an additional 90 days by a request to extend the preservation." (p. 11)	Sample preservation request asks AOL to preserve data for 90 days. (p.11)	Does not say	eBay keeps most account records indefinitely and transactional records for two years. PayPal keeps all records indefinitely (p. 1)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	YAHOO!	AOL	craigslist	eBay PayPal
Is content that has been changed or deleted by user (including private messages) still available?	"Yahoo! will be unable to search for and produce deleted material, including email and Group posts, unless such requrest is received within 24 hours of the deletion and is specifically requestsed by prior legal process. In most cases where deleted content is requested, Yahoo! will seek reimbursement for any engineer time incurred in connection with the request." (p. 7)	Does not say whether deleted email can be recovered	Does not say	Does not say
Can law enforcement monitor user account without user knowledge?	Does not say	Does not say	Does not say	Does not disclose law enforcement inquiries to account holders (p. 1)
Does site have exception for emergency disclosure?	"Yahoo! Is permitted, but not required, to voluntarily disclose information, including contents of communications and customer records [. . .] if Yahoo! believes in good faith that an emergency involving imminent danger of death or serious physical injury to any person requires such disclosure without delay." (p. 12) • Emergency disclosure request has set of seven questions: Nature of emergency? Who is threatened? What is nature of threat? Why would normal disclosure be insufficient? What info is needed? Explain how info will avert threat? Attach any electronic evidence of threat? (p. 16)	"The Stored Communications Act permits an Internet service provider to disclose the content of electronic or wire communications or customer records to law enforcement 'if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure withouot delay of communications [or records] relating to the emergency.'" "In the event of an emergency, please telephone AOL's Public Safety and Criminal Investigations unit at [redacted] and provide us with specific facts concerning the emergency that you believe requires immediate disclosure of communications or records relating to the emergency." The specific facts should include: description of the emergency, explanation that the danger is imminent, what specific records are needed (p. 13)	Does not say	Has a "First Responder" service that can return calls within 24 hours and process complaints quickly (pp. 1-2)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	YAHOO!	AOL	craigslist	eBay PayPal
Does site charge law enforcement fees?	Federal law "requires law enforcement to reimburse providers like Yahoo! for costs incurred responding to subpoena requests, court orders, or search warrants." Lists a fee schedule: • Basic subscriber records: "approx. $20 for the first ID, $10 per ID thereafter" • Basic Group Information (including information about moderators): "approx $20 for a group with a single moderator" • Contents of subscriber accounts, including email: "approx. $30-$40 per user" • Contents of Groups: "approx. $40-$80 per group" (p. 12) • Also, where deleted content is requested, Yahoo! will seek reimbursement for any engineer time incurred in connection with the request." (p. 7)	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	Sent by fax (p. 11)	Signed fax on department letterhead with law enforcement ID (pp. 11-12)	"Official requests for release of records can be submitted by email, fax, or mail."	Signed fax on department letterhead for user contact info, subpoena, court order, or search warrant requierd for full records (p. 2)
Does site address fake accounts created by law enforcement?	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Can get user consent (p. 13)	Will release data upon user consent through form (p. 14)	Does not say	Does not say
How will site deliver data?	Unclear how Yahoo! delivers information	mail (p. 8)	Can respond via fax, email, or mail	Provides records electronically, via secure website, or CD via Fed Ex (p. 1)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	YAHOO!	AOL	craigslist	eBay PayPal
Other info?		Contains a search warrant directory page, listing fax numbers for fed and military warrants, state or local agencies, and particular jurisdictions, including California, Florida, Minnesota, Washington (state), New York (p. 10) The site also has a three paragraph description of BEBO searches and the information it can provide to LE (p. 19)	The guide is a page from Craigslist's website: http://www.craigslist.org/about/help/subpoenas_and_search_warrants	• Law enforcement must provide a minimum of name, email address and User Name (for eBay investigations) to locate the correct account. (p. 1) • Turnaround time for requests is typically 10-15 business days (p. 2) • but Ebay/PayPal make" listing and member information immediately available to law enforcement via Leadsonline's First Responder Service." (p. 1)
Sample forms or sample language?	Yahoo! provides sample preservation request letter (p. 14), sample language for subpoenas, court orders, and search warrants (p. 15), emergency disclosure request (p. 16), and sample consent form (p. 17)	Sample subpoena language and subpoena format requirements (pp. 7-8), sample search warrant (p. 9), sample preservation request (pp. 11-12), emergency voluntary disclosure request (p. 13), user consent form (p. 14)		

	photobucket	myYearbook	NING	STICKAM	TAGGED	imvu
Date	**Undated**	**April 2010**	**July 2009**	**April 26, 2010**	**Undated**	**Undated**
Date, length, link (if available) and other info	Undated, eight pages	April 2010, four pages	July 2009, four pages	April 26, 2010, 16 pages	Undated, 16 pages	Undated, 2 pages
How does Guide address Legal Process Requirements under Electronic Communications Privacy Act (ECPA)?	"The types of process necessary to permit Photobucket to produce each category of information under the SCA differs only slightly." • subpoena for "first name, last name, user/screen name, ZIP code, country, email address, account creation date/time" • subpoena for "Date and IP for most recent account access, Registration IP, Banned date/time (if account banned), Date/Time of Upload or Modification of file, Upload IP for files uploaded after June 1, 2007" • court order, search warrant, or subpoena where governent provides prior notice to subscriber for "image and video content in a user's account" (pp. 3-4)	• No legal process required for "Public Information," such as profile page, profile images. • *subpoena* for "General Information," including user name, user ID, DOB, age, location (if known), school (if known), email address, password, date joined, user name changes, DOB changes, violations of terms of service, IP logs of last 6 months (login times only), IP addresses, date and time logged in, all profile pictures in account (though accounts deleted by MYB or the user willnot have any images available) • *search warrant* for "Communications/private Information," including private messagees, instant messages, embedded images in messages. (pp. 1-2)	"Ning can provide you with the following information once we receive a subpoena, search warrant or court order" • *subpoena* for the registration email of the Network Creator and Members who uploaded the content, registration IP addresses, Usernames, credit card information (if any) • *search warrant* for all images and videos of suspected child pornography, date/time stamped IP addresses at time member uploaded content in question, any and all messages received from creators and members, subject line and date/time stamp of all automated email notifications (pp. 2-3)	Non-public information requires legal process in compliance with ECPA	"To request private (non-public) information from Tagged about a specific profile or user, we requires a subpoena, search warrant or other legal process. The following list is private content that is not publicly accessible" • "IP logs (recorded at time of login), Date profile created, Dates and times of login (PST), E-mail address provided by user, ZIP code provided by user, Name provided by user, Screen Name, Private Messages" • "The following are only retained if the user has not deleted them from their page: Confessions, Boxxes, Journals." (p. 6)	• *subpoena* for "basic account information" will include "avatar name, e-mail address, customer ID (all unique) as well as the IP address used to register the account and any device fingerprints on file [. . .] If account communications are requested, IMVU will provide the text of web-based messages and a summary of realt-time chats (via IMVU's 3D client) that will include the accounts participating in chats but not the actual text of the chat" (page 1)
How does site define and/or distinguish different types of user information	Basic user (subpoena): name, user name, ZIP code, country, email, account creation date (p. 4) IP logs: subpoena, court order, search warrant or user consent (p. 4)	Public info available without legal process: Profile page, profile images; General info (subpoena): user name, ID, birthday, age, location password, date joined, changes to profile, IP logs, profile pictures (pp. 1-2) Communications (search warrant): private messages, instant messages, any images embedded in messages (p. 2)	Subpoena: email, IP address, username, credit card information (if available) (pp. 2-3) Search warrant: Images, videos, IP address, all messages (p. 3)	Subpoena required for basic user information, log-in information, and stored files (p. 4) Court order required for full access to profile; search warrant required for private user messages (p. 4)	Subpoena: IP logs, date profile created, dates of login, email address, ZIP code, name, screen name (p. 6) Unclear what level of legal process is required for messages (p. 6)	Basic account information (subpoena): avatar name, email address, customer ID, IP addresses and device fingerprint (p. 1) Unclear what legal process is required for text of web messages and chat logs (p. 1)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	photobucket	myYearbook	NING	STICKAM	TAGGED	imvu
What other info is available?	Images and video available by subpoena if subscriber given notice; available with court order or warrant otherwise (p. 4)	Does not say	Images available with search warrant (p. 3)	Video, audio, and photo files available via subpoena (p. 2)	Not clear what level of legal process is required for this information	Does not say
How does LE Guide address IP and other logs?	IP logs: subpoena, court order, search warrant or user consent (p. 4)	Can be produced with subpoena (p. 2)	IP addresses can be produced (p. 3)	IP logs available with subpoeana (p. 1, 4)	IP logs are available with subpoena (p. 6)	Does not say
How long is data generally retained? How long in reponse to preservation request?	Data is retained one year; will preserve files requested for 90 days (p. 4)	Active accounts kept indefinitely, IP logs retained for 6 months (p. 3)	90 days unless preservation request has been made (pp. 1-2)	Most data retained 90 days but will be retained longer if given a preservation request (p. 3)	"Tagged retains information on its users for certain periods of time. […] To the extent information that was scheduled to be deleted needs to be retained by Tagged due to an on-going law enforcement investigation, Tagged will do so in response to a written law enforcement preseration request." • IP logs "are saved for 6 months" • Private messages "are retained until the user removes them. Tagged may be able to recover them if the sender's Tagged User ID or email address is provided." • Sent Mail "is only retained if the user saves their outgoing messages." • Trash Mail "(mail that has been read and discarded) is retained 30 days or less." • Deleted Accounts "mail is available for deleted accounts with the same rules as active accounts." (pp. 7-8)	"IMVU does not have a policy for the regular purging or removal of account records but communication data may be missing or incomplete after 6 months." (p. 1)

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	photobucket	myYearbook	NING	STICKAM	TAGGED	imvu
Is content that has been changed or deleted by user (including private messages) still available?	Active users can delete files from account (p. 4)	• Describes that "accounts which have been deleted by either MYB staff or the user will not have any images available." (p. 3) • "Accounts which have been deleted by MYB staff or deleted by the user cannot be seen on the site. Like active accounts, all information is still available except for profile pictures." (p. 3) • Does not say regarding private messages. • Regarding instant messages "No general records are kept on instant messages. If a member is reporting a violation of TOS, the conversation is saved and provided to MYB. Those IM conversations are retained."	Does not say	• Active users can modify and delete account infomration and files (p. 3) • Does not say whether there is a different retention schedule for email messages	• Users can delete or modify information (p. 7) • Mail is retained until user deletes the messages, though undeleted mail can be accessed after users delete accounts with Tagged (p. 7)	Does not say
Can law enforcement monitor user account without user knowledge?	Does not say	Does not say	On discovery of illegal activity, account is disabled and member is informed that law enforcement have been contacted (p. 2)	Does not say	Once preservation request is received "the account will still be publicly viewable, the user will not be able to log into his/her account, information in the Sent Mail/Trash folder is still subject to automatic deletion." "If restricting the user's access to the profile will impede and investigation, you may request that private messages be output to a flate file for peservation before a subpoena is served.You must specifically request in the letter that the user not be notified of the investigation if you do not want the subject account to be locked." (p. 8)	"In the legal documentation please be specific if the account should remain enabled. If IMVU becomes aware of an account with suspicious or illegal activity it will likely be disabled. If leaving an account enabled will assist in an investigation, please make sure this is stated when submitting the subpoena, search warrant, or other court-ordered demand." (p. 2)
Does site have exception for emergency disclosure?	"Photobucket will also exercise its discretion under the SCA to release information without legal process where an imminent threat of death or serious physical injury to a person exists that necessitates disclosure" Asked to provide information on the nature of the emergency, the name of the person who is threatened, the specific information in Photobucket's possession related to the emergency. (p. 5)	Does not say	Does not say	Can release when it "believes in good faith that an emergency involving danger of death or serious physical injury" (p. 4)	Does not say	Does not say

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	photobucket	myYearbook	NING	STICKAM	TAGGED	imvu
Does site charge law enforcement fees?	Does not say	Does not say	Does not say	Does not say	Does not say	Does not say
What are the requirements to begin preserving records?	Correspondence must include contact information where files will be sent (p. 6)	Faxed requests (p. 1)	Requests involving legal process must be sent via fax and certified mail (p. 1)	Correspondence must identify officer and information sought (pp. 4-5)	Faxed letter on department letterhead (pp. 6, 13)	When requesting account data, subpoena or search warrant are required (p. 2)
Does site address fake accounts created by law enforcement?	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts	No warning about deleting fake police accounts
Can user consent to data release?	Can get user consent (p. 4)	Will accept user consent (page 3)	Does not say	Does not say	Can get user consent (p. 14)	Does not say
How will site deliver data?	Delivered via CD (p. 6)	Does not say	Can send via mail (p. 2)	Delivered via email (p. 5)	Looks like it is delivered electronically (pp. 10-11)	Does not say

SOCIAL MEDIA—A Guide to the Law Enforcement Guides

	photobucket	myYearbook	NING	STICKAM	TAGGED	imvu
Other info?	• The guide lays out how it reports accounts containing child pornography, using NCMEC Reporting. (p. 5) • The guide contains an FAQ for law enforcement along with information on how the data it sends to LE is formatted (pp. 6-7) • This guide has what appears to be the same reference sheet obtained in either the 2005 or 2007 MySpace guide (p. 8)	MYB takes a snap shot of the site every night and is kept on a backup file for 7 days. After 7 days, the file is deleted. MYB also keeps the file taken on the last calendar day of the month for two months before deleting it. (p. 4)	Ning's guide is particularly directed toward the discovery of child pornography, outlining NCMEC Reporting requirements, as well as outlining ways internationa jurisdictions can use ECPA to get information (p. 3) Ning also says that if LE wants child pornography mailed to it, it must directly mandate so in the search warrant, as Ning does not want to be prosecuted for transmission of child pornography (p. 2)		Guide contains a page devoted to "Understanding IP Addresses" (p. 15) and a page with "Websites and Resources" for LE (p. 16)	• Disclaimer that IMVU does not verify customer data (p. 1) • If request is related to ID theft, victims can request information without a subpoena or warrant (page 2)
Sample forms or sample language?	Language for preservation and emergency requests (pp. 4-5)				sample subpoena (p. 12), sample preservation request letter (p. 13), sample consent form (p. 14)	Guide instructs that "When requesting account data, please have the subpoena or search warrant request: 'Account data for the account(s) matching the Avatar name, e-mail or IP addresses *[insert known data here]* and for any account(s) that appears to be controlled by the same person." (p. 2)