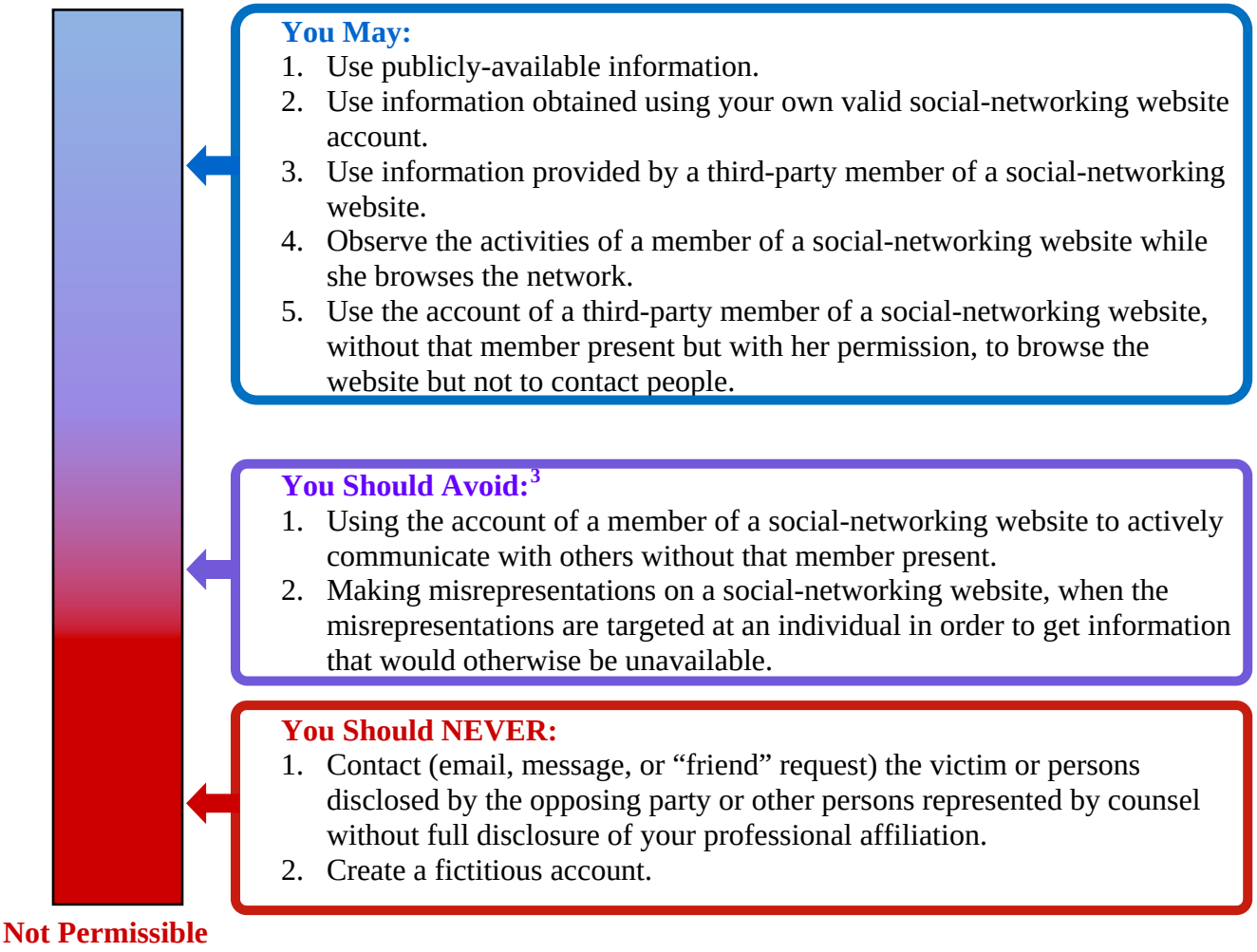
Handbook on Conducting Research on Social-Networking Websites in California[1]

Created by
David Lee and Shane Witnov[2]
Samuelson Law, Technology & Public Policy Clinic, UC Berkeley School of Law
for
The Santa Clara County Public Defender's Office

Overview

In conducting research on social-networking websites,



---

[2] Under the supervision of Supervising Attorney Jennifer Lynch.

[3] "Avoid" means you should not use any of the listed methods except as a last resort, with careful consideration of the consequences, in consultation with the supervising attorney.

Introduction

Investigators are limited in their use of social-networking websites[4] for research by a number of different factors including state and federal law, the website's terms of use, and ethical rules.[5] This handbook uses the term "investigator" broadly to include attorneys or anyone working under an attorney.[6] At times, ethical and legal restrictions are unclear and the value of the information to be obtained should be weighed against the potential consequences in consultation with the team investigating the case. Generally, a conservative approach should be adopted to ensure legal compliance, preserve the goodwill of the courts and opposing counsel, and to maintain high ethical standards.

You May:

1. Use publicly-available information

An investigator may always access publicly-available information. Publicly-available information is information on the internet that can be accessed without needing to log in. Information found through a search engine as well as information on a social-networking website that can be accessed without logging in is publicly-available information.

For example, an investigator may use a search engine, like Google, to search for the name of a person of interest. Often, the search result will return a link to the person's social network webpage. Viewing information returned from this type of search does not violate any ethical or legal rules. Furthermore, many profiles on MySpace are publicly accessible. An investigator could use a search engine or the MySpace search, without logging in or having an account, to find and access publicly available profiles.

2. Use information obtained using your own valid social-networking website account

An investigator may create an account on a social-networking website, with accurate information, and conduct any research she wishes to on that network. An investigator may ask to join groups and access the profiles of people that are enabled by joining the group. The investigator may even ask an individual to be her "friend" (for example, on Facebook) as long as the person is not a witness disclosed by the opposing party or represented by counsel.[7] Because the social networking websites' terms of use

---

[4] MySpace and Facebook are two of the most widely used social-networking websites and were researched for writing this handbook.

[5] *See, e.g.*, Cal. Penal Code §1054.8, 18 U.S.C. §§ 2701-2711, MySpace Terms of Use, (June 25, 2009), http://www.myspace.com/index.cfm?fuseaction=misc.terms, Cal. Bus. & Prof. Code §§ 6068, 6106, 6128.

[6] For the purposes of this handbook, attorneys and those working under them are all considered to be bound by California Rules of Professional Conduct in additional to generally applicable law. "An attorney is responsible for the work product of his employees which is performed pursuant to his direction and authority." *Crane v. State Bar*, 30 Cal. 3d 117, 122-23 (1981) (finding attorney responsible for actions of his employees that violated the Rules of Professional Conduct).

[7] Cal. Penal Code Section 1054.8 prohibits an investigator or lawyer from interviewing, questioning, or speaking to someone disclosed as a witness by the other side unless she first clearly identifies herself, her employer and whether she represents the defense or prosecution. California Rule of Professional Conduct 2-100 prohibits communicating "directly or indirectly about the subject of the representation with a party the member knows to be represented by another lawyer in the matter." Making contact with an individual

generally require users to "not provide any false personal information,"[8] the profile should include the investigator's current employer and job title if the investigator is going to make friend requests in their official capacity.

If the person is the victim or a witness disclosed by the opposing party, the investigator may still ask to be an individual's "friend" as long as she is careful in the "friend" request to clearly identify herself and the agency she works for and to state who she represents.

3. Use information provided by a third-party member of a social-networking website.

If the client or another member of a social-networking website provides an investigator with information obtained from a social networking website, the investigator can use that information. This information could include printouts or digital copies of profile pages, communications between members, photos, or any other information accessible to the member on the social networking website.

An investigator should not encourage the client or other member to engage in deception on her behalf in order to acquire information. However, as long as the investigator did not engage in or encourage the deception, she should be able to use the information without violating any ethical duties.

4. Observe the activities of a member of a social-networking website while she browses the network.

An investigator may ask her client, a friendly witness, or someone else to come to her office to browse a social networking website. As long as the member gives permission, the investigator can observe and direct her browsing. The investigator may also ask the member to save or print information as she comes across it.

Because the investigator is merely requesting that the member browse in a certain way, she is not impersonating anyone or engaged in deceit. This method is probably the best way to obtain information that is not publicly available since no deceit is involved.

5. Use the account of a third-party member of a social networking website, without that member present but with her permission, to browse the website but not contact people.

An investigator may use the account of her client, a friendly witness, or someone else to passively browse a social-networking website when given permission by the account holder. Passively browsing means the investigator may search for and look at any profiles available to the member's account she is borrowing. However, she should not message, email, friend request, or in any other way directly communicate with anyone one else using the borrowed account.

By signing in to the social networking website, the investigator is to some degree representing herself to be a different person. Therefore, this technique should only be used if the previously discussed ones are not available. In particular, this technique may be appropriate if the client is in custody and thus unable to use the internet.

---

on a social networking site, such as asking to be that person's "friend" through Facebook, could be considered "speaking" to that person although there is no case law on the subject.

[8] Facebook Terms of Use, (Aug. 28, 2009), http://www.facebook.com/terms.php.

You Should Avoid[8]:

1. **Using the account of a member of a social-networking website to actively communicate with others without that member present**

An investigator should avoid using another social-networking website member's account to directly communicate with others via email, messaging, friend requests, or any other means. Ideally, she should only observe while the owner of the account browses the network (as described above). Using someone else's account could be considered a violation of the terms of use for many social-networking websites.[10] Furthermore, if the investigator contacts another person directly using the false identity, this may constitute deception or impersonation and be an ethical violation.[11] There are also other risks of civil and criminal penalties, albeit remote risks.[12]

2. **Making misrepresentations on a social-networking website, when the misrepresentations are targeted at an individual in order to get information that would otherwise be unavailable**

An investigator should not misrepresent herself on a social-networking website in order to get information that would otherwise be unavailable. The terms of use forbid members from misrepresenting themselves.[13] Furthermore, the ethical rules binding lawyers and those working under them generally forbid misrepresentations.[14]

Misrepresentations could include omitting relevant information from an investigator's profile, especially the investigator's current job and title.[15] Because the terms of use require users to "provide their real names and information,"[16] the profile should include the investigator's current employer and job title if the investigator is going to make friend requests. It might be considered a misrepresentation if the investigator omitted employment information and then a person of interest accepted a friend request thinking the investigator was not involved in the legal case the member was involved in. An investigator may also be tempted to lie about her city of residence or schools to gain

---

[9] *See* note 3, *supra.*

[10] For example, Facebook's terms of use say "You will not provide any false personal information on Facebook . . . You will not share your password, let anyone else access your account . . . You will not transfer your account to anyone without first getting our written permission." Facebook Terms of Use, (Aug. 28, 2009), http://www.facebook.com/terms.php. MySpace's terms of use say "You agree not to use the account, username, email address or password of another Member at any time or to disclose your password to any third party." MySpace Terms of Use, (June 25, 2009), http://www.myspace.com/index.cfm?fuseaction=misc.terms.

[11] Cal. Bus. & Prof. Code §§ 6068, 6106, 6128 prohibit deceit and dishonesty, while requiring that lawyers only use means consistent with the truth.

[12] While this may technically be a violation of the terms of use, the provisions are infrequently enforced and would likely only be a contract violation. However, there have been attempts to bring charges under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) for violating terms of use although these have generally been unsuccessful. *See*, *U.S. v. Drew*, 2009 WL 2872855, (C.D. Cal. Aug. 28, 2009), *available at* http://www.volokh.com/files/LoriDrew.pdf.

[13] Facebook's terms of use requires that all information provided be "accurate, current and complete." MySpace's terms of use similarly requires that information should be accurate.

[14] The California Business and Professional Code orders attorneys to use "means only as are consistent with truth." Cal. Bus. & Prof. Code § 6068.

[15] The investigator's role as investigator is so central to her use of the social network profile, that omission could be seen as a misrepresentation under Cal. Bus. & Prof. Code § 6068.

[16] Facebook Terms of Use, (Aug. 28, 2009), http://www.facebook.com/terms.php.

access to other networks. While these may be minor misrepresentations, they are carefully targeted deceptions to gain access to information that would not otherwise be available. Targeted misrepresentations are probably unethical.[17]

You should NEVER:

1. **Contact (email, message, or "friend" request) the victim or other persons disclosed by the opposing party or other persons represented by counsel without full disclosure of your professional affiliation**

California Penal Code section 1054.8 prohibits an investigator from communicating with the victim or any potential witnesses identified by the prosecution without identifying herself, the full name of her agency, and that she is working for the client. Asking someone to be your friend on a social-networking website without disclosing all of the required information in the friend request would probably be a violation of the statute. Emailing or messaging such a person is also prohibited. Furthermore, an investigator should never contact anyone who she knows is represented by counsel about the matter for which the representation was obtained.[18] However, accessing publicly-available information on a victim, disclosed witnesses, or represented party is allowed as described above.

2. **Create a fictitious account**

An investigator should not create a fictitious account on a social-networking website using a fake name and other false information in order to gain access to other users' information. Such behavior involves deception and is therefore unethical.[19] Furthermore, it may be a criminal violation of the website's terms of use.[20]

[17] *See* Cal. Bus. & Prof. Code §§ 6068, 6106, 6128 for laws forbidding deception.
[18] Cal. Rules of Prof. Conduct 2-100.
[19] *See* Cal. Bus. & Prof. Code §§ 6068, 6106, 6128 for laws forbidding deception.
[20] *Supra*, note 11.