Coates' Canons Blog: Anonymous Tips: Can They Really Be Anonymous? [Revised]

By Frayda Bluestein

Article: https://canons.sog.unc.edu/anonymous-tips-can-they-really-be-anonymous-revised/

This entry was posted on April 09, 2014 and is filed under Open Government, Public Records (General)

Note: This is a revised version of my earlier post on this topic. Thanks to my colleagueJeff Welty for his help in providing a more complete explanation of the criminal investigation exceptions.

Local governments want to hear from their citizens. As one city's website says, it wants citizens to be its "eyes and ears." Digital government makes it easy for citizens to communicate with their local officials. Government websites promote telephone hotlines, web forms, digital suggestion boxes, and social media to get information on customer service, budget priorities, potholes and traffic jams, violations of city codes, and fraud, abuse, or other unethical acts by government employees or officials. To encourage candid comments, these forums often promise that information can be submitted "anonymously." Is this a promise local governments can keep?

The only truly anonymous system may be one that neither requests nor captures identifying information. If a local government actually receives identifying information, however, or has a contractual right to obtain it from an outside service, that information is a public record and must be provided upon request, unless an exception in the public records law applies.

In my post about surveys I noted that the basic definition of public record – records made or received in the transaction of public business – includes information citizens provide in response to surveys about local governments services and issues. The same holds true for information received through tips, hot lines, web reporting forms, digital suggestion boxes, and social media, including any information about the identity of the responder.

Identifying information could be subject to public access even if it is gathered through a local government's intranet or through some other process internal to the public agency. The information still fits the definition of a public record.

Examples of identifying information could include a person's name, address, or phone number, which some electronic reporting systems prompt the responder to provide. (Some systems make it optional to provide this type of information.) An email address that is provided in response to a form or other prompt would also be considered a public record. The analysis may be different, however, for an email, IP address, or other electronic identifier that is embedded in the communication, rather than voluntarily provided in response to a prompt or form. Such information may be considered "metadata," and it is unclear whether, and to what extent, public agencies are required to provide access to metadata under the North Carolina public records law. (See Kara Millonzi's posts here, and here, to read more about metadata and its status under the public records law.) Depending upon a court's analysis, identifying information that exists in metadata may be subject to public access, even if the tipster and the local government meant for the tip to be anonymous.

What about exceptions that might apply? There is no general exception in the public records law for identifying information about people who provide tips, comments, or other information to public agencies. So if an exception applies, it would be based on the subject matter involved. Two common topics, personnel information and reports of criminal activity, are subject to exceptions under the law.

Personnel information – an exception from public access: Information about the performance of an employee is part of that employee's confidential personnel file. Tips and comments about specific employees are not available to the general public. But the employee who is the subject of the tip or comment may have access to the information, including possibly the identity of the person who provided it. (See my blog post here, regarding a court case dealing with this issue.)

Law enforcement records: If a tip involves information about criminal activity, the status of identifying information may depend upon what type of tipster is involved. G.S. 132-1.4 provides that most criminal investigation records are not public records, but goes on to list certain criminal investigation information that must be made public upon request. There are

four separate provisions in the statute that address the status of information about people who provide information about crimes.

Complaining Witnesses – identifying information is public. The list of criminal investigation information that must be made public under G.S. 132-1.4 includes the name, sex, age, and address of a "complaining witness." G.S. 132-1.4(c)(6) [The statute requires temporary withholding of this information if its release is reasonably likely to cause harm to the complaining witness. G.S. 132-1.4(d).] The law defines a complaining witness as "a victim *or other person* who reports a violation or apparent violation of the law to a public law enforcement agency." G.S. 132-1.4(c)(5)(emphasis added) Although a complaining witness is typically thought of as someone who is the victim of a crime, the statute clearly expands the meaning to include general members of the public who report crimes. This provision makes public information about people who report violations of most local ordinances, since they are always enforceable as a criminal offense unless the unit of government has explicitly removed the possibility of criminal enforcement.

Emergency Calls – identity is not public. G.S. 132-1.4(c)(4) makes the contents of 911 and other emergency calls public, but excludes from public access any content that reveals the identity of a caller, victim, or witness. This provision is confusing in light of the provision in this same statute, which makes complaining witness information public. It apparently means, however, that complaining witnesses information can remain anonymous if it is obtained only through the 911 or other emergency call system.

Crime Stopper Organizations –identity is not public. G.S. 132-1.4(h)(1) provides that a law enforcement agency need not disclose any information that would not have to be disclosed under Chapter 15A (which governs the rules of discovery in criminal cases). G.S. 15A-904(a3) exempts from the discovery requirements the identity of individuals who provide information to a "Crime Stoppers" or similarly named entity, as defined in the statute. This means that crime stopper systems that meet the definition in the statute can promise anonymity.

Confidential Informants – identity is not public. G.S. 132-1.4(h)(2) provides that a law enforcement agency is not required to disclose information reasonably likely to identify a "confidential informant." This term is not defined in the statute, but is generally understood to include individuals (usually criminals) who have an arrangement with a law enforcement agency to provide information in exchange for favorable treatment in their cases. It is possible that a court might interpret this provision as protecting other members of the general public who provide tips under a general promise of confidentiality. Such an interpretation, however, may be difficult to reconcile with the broad definition of "complaining witness" which requires the release of identifying information about informants who are members of the general public.

Local school administrative units – a specific exception: A statute that applies only to local school administrative units, G.S. 115C-105.51, authorizes the establishment of "an anonymous tip line, in coordination with local law enforcement and social services agencies, to receive anonymous information on internal or external risks to school buildings and school-related activities."

These exceptions provide limited authority for anonymous tips. In other cases, the only way to protect the identity of tipsters is to avoid obtaining the information. The exceptions in the statutes recognize the value of anonymity, especially in the criminal investigation context. On the other hand, sometimes citizen information is necessary in order to follow up, verify information, or improve service delivery. Here are some options to consider when balancing the desire for information, the value of anonymity, and the benefit of being able to follow up with a citizen:

- Don't ask for identifying information, and use a system that does not capture metadata. (It's my understanding that there are some products that do not capture the metadata from a respondent.) This approach avoids the problem by preventing the agency from receiving the identifying information. Of course, not having the information may hinder efforts to respond to or solve the problem that is reported.
- Make it optional to provide identifying information, and provide clear notice that if it is provided, it may be subject to release under the public records law.
- Use separate portals for collecting different types of information. For example, set up a telephone or other secure and anonymous hot line for sensitive and serious tips, such as those involving criminal activity, fraud, or employee misconduct. In these cases, people are more likely to report it if they know it's anonymous, and having the information may be more important than knowing who is providing it. For less sensitive issues – such as reporting service problems and concerns, or making suggestions for improving services – use a digital (or physical) suggestion box, an email system, or web form that captures or provides the option to include identifying

information. In these cases, follow up may be necessary, and customer service may be improved with a return communication. These sites should make it clear that identifying information may be subject to public access if requested.
- Contract with a third party to collect the information. But note that if the contract allows the public agency to have access to the identifying information, it may still be subject to public access under the law. (See, David M. Lawrence, Public Records Law for North Carolina Local Governments, pp. 24-25.) A contract could be structured to allow the local government limited access to individual information, for example, only upon request and with the consent of the individual with full disclosure that the information may be subject to public access. Information about individuals who do not consent would remain anonymous.

What systems are North Carolina local governments using to make the public your “eyes and ears”? I’d love to hear from you about solutions you’ve used. (But I can’t promise that your comments will be anonymous.)

Links

- nccriminallaw.sog.unc.edu/
- www.cityofboston.gov/doit/apps/citizensconnect.asp
- www.raleighnc.gov/home/content/Police/Articles/OnlineCrimeReporting.html
- www.tipsubmit.com/WebTips.aspx?AgencyID=1019&HR=http://www.tipsoft.com/index.aspx?p=webtips
- charlottenc.gov/pages/contactus.aspx
- canons.sog.unc.edu/?p=3677
- canons.sog.unc.edu/?p=1984
- canons.sog.unc.edu/?p=2064
- canons.sog.unc.edu/?p=7059
- www.ncga.state.nc.us/gascripts/statutes/statutelookup.pl?statute=132-1.4
- www.ncga.state.nc.us/gascripts/statutes/statutelookup.pl?statute=15A-904
- www.ncga.state.nc.us/gascripts/statutes/statutelookup.pl?statute=115C-105.51
- www.sog.unc.edu/publications/books/public-records-law-north-carolina-local-governments-second-edition