Dude, Where's My Data? Privacy and Information Security for Musicians and Fans

By Adam Holofcener and Liz Allen

Future of Music Coalition, August 9, 2011
www.futureofmusic.org

I. Why Does Privacy Matter?

Everyday brings new concerns about data in the online realm. From high-profile hacking incidents to issues around the use of personal information, our migration to digital platforms has tested traditional conventions around privacy. These developments also affect musicians and fans, especially as music is increasingly accessed via mobile devices, "apps" and social networks.

Future of Music Coalition has always been interested in issues at the intersection of music, technology, policy and law. So, while we may not have the expertise to "solve" the issue of privacy in digital music (and we're hardly alone there), we do feel that we have enough of a stake to join the conversation. This article will hopefully be useful to those who have questions, concerns or are just plain curious about where the issue may be heading. To a large degree, we'll be focusing on the mobile space, due to the explosion of popular music-related apps.
Among other things, the development of the internet has allowed artists to connect directly with fans. This is very different from previous versions of the music business, where musicians' access to audiences was limited and tightly controlled. Today's digital environment allows both established and developing artists to do everything from market and sell product to route tours to build anticipation for upcoming releases, appearances and more. Much of this is accomplished through the collection of certain information. We also recognize that the ability for digital services to make money from user data could go some way towards attracting greater investment in music.

Large-scale data collection can be extremely beneficial to leverage fan interest in the most efficient and effective manner possible. Likewise, technology platforms harvest user data to create revenue beyond their core services. Yet many musicians and fans have yet to consider what such activity means for individual privacy and information security. Some artists are certainly ready to start asking the question, however. At the 2009 Future of Music Policy Summit, musician Erin McKeown voiced concerns about data collection that have only become more relevant as technology progresses. McKeown isn't entirely comfortable when websites and applications collect and use information based on her internet browsing. She is even more

worried about sites that she directs her fans to which may have dicey data collection practices. What should the standards be for collecting third-party user information? How much transparency in data collection policies is appropriate? How is the data shared, and with whom? What is the tradeoff between investment, utility and informational security?

We know that some data collection is reasonable and consumer friendly — who doesn't like it when Amazon recommends what else you should buy with that DeVotchKa record? Still, with so many uncertainties around data collection, we thought it prudent to examine privacy and technology as it applies to musicians. We hope this aids artists in their cost-benefit analyses when it comes to choosing potentially useful applications and services.

We will begin by examining privacy policies in terms of their basic structure and scope. Clearly, our review is not meant to be comprehensive, but we hope to give readers a better sense of the landscape. Second, we will explore the practical impact of these policies on users. Finally, we will offer some constructive options to consider for musicians who are concerned about their online privacy and that of their fans.

II. Current State of Privacy Law

At present, US privacy law is very fragmented and confusing. Even the definition could benefit from clarification. Generally speaking, "privacy law" is an umbrella term that covers many different areas — everything from how the government collects and manages personal information to Constitutional restrictions on laws regulating individuals' private lives. For the purposes of our discussion, we will focus on personal privacy online: what protections are in place for individuals' personal information as they interact with companies, other users and anyone else they may encounter on the internet.

Personal privacy protections online are further divided into those governing internet use by children and those that apply to adults. Websites and apps that target young children are regulated by laws like the Children's Online Privacy Protection Act (COPPA), which restricts the types and amount of information these websites can collect about their minor users. For adult users, however, there are no federal legal protections in place. Instead, the privacy framework is made up of a patchwork of state laws and some industry "best practices" that are essentially suggestions for self-regulation, not actual legal rules.

Without federal laws protecting user privacy online, can websites do whatever they want with regard to their users' information? The answer is "sort of," and this is where things get tricky. Some states, for instance, have laws that dictate how websites may use information collected from individuals who are residents of that state. Utah and California require businesses (both off- and online) to disclose to customers, in writing, the types of personal information it shares or

sells to third parties for direct marketing purposes or for compensation. Some states also require websites to have (and abide by) privacy policies with certain baseline requirements, such as listing exactly what information the site shares with third parties. Other states, however, don't have any online privacy protection laws at all.

As for federal regulation (rules that everyone in the US must follow), Congress seems to be hesitant to enact privacy laws that would regulate the way private companies collect, store and interact with adult internet users' information. In the meantime, the Federal Trade Commission (FTC) has limited power to look out for personal privacy online. The FTC can hold industry actors accountable for violating promises made to individuals in their privacy policies. If a website has a privacy policy, and then violates that privacy policy, the FTC can challenge the entity who owns the website and protect users. Of course, this also means that if a website doesn't have a privacy policy, the FTC is powerless to challenge even outrageous information sharing, storage or sale practices by that site.

Despite a lack of legal consistency, some industry standards, including those adopted by many website operators on a voluntary basis, have evolved. Several organizations issue "badges" or "certifications" for websites they believe meet favorable privacy standards. There are different variations of industry standards, but they are all generally based on the Organization for Economic Cooperation and Development (OECD) guidelines established in 1980. Note that the OECD principles are "guidelines" — not actual laws — so private entities that operate websites don't have to obey them, and the FTC has no power to force them to do so. Still, the guidelines provide a helpful framework for websites that wish to protect their users' information, and they continue to shape the way policymakers think about online privacy when proposing new legislation or other regulations.

The OECD guidelines assert that an effective online privacy policy must take into account eight important principles: (1) collection limitation (website operators should limit the collection of personal data and that data should be obtained by lawful and fair means with the knowledge of individuals, if possible); (2) data quality (information collected should be relevant to the purposes for which it is to be used and should be accurate, complete and up-to-date); (3) purpose specification (the operator's purpose for collecting specific information should be determined before the time of collection and use of that data should be limited to that specified use); (4) use limitation (information should not be disclosed, made available or otherwise used for purposes not previously specified, except with consent of the individual or to comply with the law); (5) security safeguards (operators should protect personal information using reasonable security safeguards); (6) openness (operators should have a policy of openness about developments, practices and policies with respect to personal information); (7) individual participation (an individual should be able to obtain confirmation of whether or not the website operator has

information relating to him); (8) accountability (website operators should be accountable for complying with these principles).

Ultimately, there is no specific recourse for individual internet users who feel a website operator violated their privacy. Individuals may send a complaint about a website operator to the FTC, and the FTC may bring a case if it believes the operator engaged in unfair or deceptive practices (e.g., if the site violated its own privacy promises to its users in accordance with the site's privacy policy). If the FTC deems a website's information practices illegal, it may issue an injunction against those practices, forcing the site to comply with higher privacy protection standards. If Congress doesn't enact a statute allowing the FTC to create privacy rules, there is nothing more the FTC can do. This leaves the collection of personal information by private website operators largely unregulated by the government, with many privacy judgments left in the hands of the industry itself.

Keep in mind that the privacy laws, regulations and concepts mentioned so far have been geared toward websites that individuals access through computers or internet browsers via a traditional online connection. An ongoing debate asks whether the same privacy practices and standards should translate to mobile information collection on other electronic devices, as well as the applications that run on these platforms. As this article largely focuses on the latter environment, our analysis in many ways is even more uncertain. Nevertheless, we'll do our best to analyze this evolving landscape.

III. Privacy Policies

a. What do They Contain?

Privacy policies come in all shapes and sizes — from painstakingly comprehensive to entirely absent. With that being said, this article should not be used as a "how to guide" to privacy policies, nor should it be taken as a critique of any examples given — although we can say that one red flag would be if an application completely lacks a privacy policy. This section will look at what some privacy policies say, and don't say, using example applications that working musicians are likely to use.

People can access music on their mobile devices in a host of different ways. Here, we are primarily interested in the privacy implications of mobile apps that involve creators putting up their own work and then asking their fans to access the work via their mobile phone. This brings applications like Bandcamp and Soundcloud to mind. Musicians also ask fans to interact with apps that deal more concretely with sensitive information such as Square, a credit card processing app that allows for transactions to take place via mobile phone. Later we'll take a look at specific language from privacy policies. For now, we'll try to shed light on several basic

privacy questions: who is collecting data, what data is being collected and what can that data be used for?

Theoretically, there are two flavors of privacy policy: that of a website and that of an application used to access information and services on the website. It is an entirely different question as to whether, or even how, these policies fit together, but it is worth mentioning that there may always be multiple layers of interacting — or contradicting — policies at play with your use of a particular mobile app. So, the first question of "who is collecting data?" can have multiple answers: no one, the website that you are accessing through your mobile device, the manufacturer of the mobile application that you are using or all of the above. It is best to assume that every intermediary that participates in helping you utilize a particular app has collected some data from you in the process. This is not necessarily a bad thing, as we will see when we look at what data applications and websites actually collect.

Privacy policies primarily address two types of data collection: personally identifying information (PII) and non-personally identifying information (NPII). These terms are defined by the companies who run the specific websites and applications; however, there is a set of generally used terms which typically fall into one of the two categories. Things like your name, credit card number, email address, home address, phone number, picture and website URL are usually considered PII. However, there are some discrepancies as to whether data such as your location are PII or NPII. After identifying what information falls into which category, privacy policies outline what they intend to do with each type of data set.

What companies do with your information again falls into two basic categories: using your information to run the website in the most effective and efficient way and exploiting the data for its own sake. Usually, PII can only be used to run the services offered through the website or application — this includes sending information to third parties if necessary (picture a payment processing app needing to send your credit card info to a bank to process a payment). If websites or applications want to share your PII with third parties for other reasons than the general operation of services, their policies may require your permission. For NPII, the trend is that most companies may stipulate in their privacy policy that they may provide that data to third parties after the information is aggregated and made anonymous. One thing to remember here are that there is a discrepancy between what may be considered PII and NPII. Another is a company's accountability to their declared polices. Lastly, there is the level to which NPII can be made anonymous, even in the aggregate.

Two ancillary points are worth making as well. Privacy policies generally say that they are subject to change at any time without warning; typically, they give a "last updated" date and it is worth re-checking privacy policies every so often. Second, privacy policies that say they will not sell or rent your information to other organizations usually stipulate that the data is itself an asset

of the company. This means that, on the occasion of the sale of the business, data may in fact be sold along with the company. A question on this latter point, therefore: what if a credit card processing company decides to sell itself entirely, including its data, to a company that is not another credit card processing company but rather a different kind of company entirely, such as a data mining company?

At the end of most privacy policies, the website or app acknowledges that you, the consumer, may opt-out of giving the entity your information; however, that opt-out is sometimes contingent upon you receiving less than optimal service from the app or, sometimes, asking you to not use the app at all. So, with privacy policies being opt-out, subject to change and malleable depending on ownership of the company, it pays to stay abreast of terms for the online services that you use. In the next section we will explore specific examples of some of the types of privacy policies mentioned above.

b. What is the Practical Effect?

Because each app, website and operating systems' privacy policy is unique (or nonexistent, as the case may be), there are many issues when these different services interact with one another. This raises questions about what happens when, say, the operating system on which an app runs has a privacy policy but the app itself does not. Unfortunately, there are no simple answers to these questions, but here is our best shot at guessing how some of these issues might play out in the real world.

Perhaps the most common issue arises when privacy policies provide different definitions for critical terms that appear in the policies of many services. The result is that Apple, for example, does not consider information like a user's location and the identification number of his personal device (phone, computer or tablet) to be personally identifying information, while privacy policies of some apps sold in Apple's App Store and that run over its operating system may specify that such information is PII. This is confusing to users who see the term "personally identifiable information" and assume it has the same meaning across privacy policies. It is even more confusing when the definition of that term seems counterintuitive, such as location and unique device ID not being considered identifying.

Another issue arises when information-sharing practices that are allowed by one service's privacy policy are prohibited by another, and an individual uses the two services in conjunction with one another. When both service providers retain their own copies of an individual's data, presumably their respective privacy policies govern each service's use of that information. It does not seem, however, that one privacy policy's terms will trump another's. For example, even though an app runs on Google's operating system (or a website is accessed through Google's Chrome browser), that app or website does not need to adhere to Google's privacy policy. In

fact, Google's privacy policy explicitly states: "information collected by Google when you enable a third party application is processed under this Privacy Policy. Information collected by the third party application provider is governed by their privacy policies." Therefore, when a user allows one service to transfer his information to a third party service, that information will now exist in two different forms and be governed by two different privacy policies. This is even more troublesome when the third party app or other service doesn't have a privacy policy at all. Which brings us to our next issue.

If a website, operating system, app or other service lacks a privacy policy, it is completely unregulated in terms of how it may uses the information it collects. If it does not make any promises to its users in the form of a privacy policy, the FTC cannot step in and force the service provider to abide by another policy or standard. As mentioned earlier in this paper, there are some industry standards that have started to evolve, but these best practices are not mandatory and there is no way to force services to adopt them. Ultimately, when individuals trust their personal information to apps and websites without privacy policies there is no guarantee they will receive any protection at all.

Some companies provide services that cover many platforms, but only provide one privacy policy across the board. SoundCloud's privacy policy, for example, claims to only govern "use of SoundCloud's internet platform at www.soundcloud.com … and any services that SoundCloud provides through this website." SoundCloud also offers an app that users can download to their mobile devices, but this app does not have a privacy policy of its own. Is the app governed by the soundcloud.com privacy policy or is it not a service provided through the SoundCloud website? Because the app is accessible through the website and presumably connects the user to content provided by the site, there is an argument for applying the website's privacy policy to information collected by the app. On the other hand, the app is not the same thing as the SoundCloud webpage, which can be accessed separately through a mobile device's browser. If the website's privacy policy does not apply to SoundCloud's app, the information a user provides to the website, www.soundcloud.com, may be handled in a drastically different way than that provided to the SoundCloud app (even when owned by the same company). While it may be counterintuitive, this disparity in privacy protection between platforms for the same service is perfectly legal under the current privacy protection regime.

IV. After the Fine Print

a. How Can You (at Least Sort of) Protect Yourself?

The first step in privacy protection is education. By becoming aware of the possibilities that exist for different types of privacy policies, there is less of a chance that you will be surprised by outcomes. Choosing mobile apps based upon their privacy policies is always a cost-benefit

analysis, and it is not inherently unreasonable — or inequitable — for apps to collect a certain amount of data from you as a musician or fan. The most important thing to focus on is your own comfort level. Choosing to not use products whose privacy policies do not align with your own personal ethics does not necessarily foreclose you from participating in today's music marketplace (although a very stringent approach may make it more difficult). If you utilize and support apps with privacy policies that you feel comfortable with there is less of a chance that your friends, family and fans will take issue with your digital presence.

Remember, you have the ability to opt-out. While it may sound like a hassle to have to contact each particular servive you use and ask them to not collect your data, it could assuage your main concerns. If opting out leads to you not using a particular mobile app, do not fret. At this point, privacy is beginning to become an aspect of product differentiation. Your choice could help to create an environment where apps with more consumer-friendly privacy policies will be more successful than those that do not. And why not ask your fans how they feel? After all, you're all in it together in this brave new world of content and information exchange.

There is always the possibility that Congress will act to clarify some of these issues. However, as we previously mentioned, there is no federal privacy law that really touches data collection online — particulary for the world of mobile apps and services. However, there may be state specific laws that apply to you and your fan base living in a particular area. It may be worth looking at those laws as you further your understanding of this subject.

Now let's look at the reality of the entire situation. Don't worry, it is not really that bleak.

b. Privacy Policies Aside, How Safe are You Online?

Ultimately, your personal information is as safe as you keep it. If you choose to use apps and other internet services based on which privacy policies protect your information best, opt-out of certain information collection schemes and are conscious about how much and what types of information you provide, you will probably be in good shape. If you're lucky enough to live in a state with some laws regulating the ways companies can use your personal information, you should be aware of these laws and know your rights. Keep in mind that most companies and app developers aren't evil. In fact, many are doing their best to build a sustainable 21st century digital music ecosystem. The absence of a privacy policy doesn't necessarily mean they want to exploit your personal information. Some independent app developers simply may not be aware that typing up a privacy policy is something they should do, and many lack the funds to employ a lawyer or other advisor to help them out. There is also something to be said for the industry best practices mentioned earlier. Many services take these principles seriously and try to strike a balance between using personal information for some activities (like advertising), while protecting personally identifiable information, as defined by that company's privacy policy.

Finally, some believe Congress may be on the verge of passing comprehensive Internet privacy protection laws. Until then, take a deep breath and stay calm: actually reading privacy policies, understanding your rights and being aware of possible dangers is your best bet. Like GI Joe says, "knowing is half the battle."

CDT – Online Privacy Guide
http://www.cdt.org/privacy/guide

CDT – existing federal privacy laws
http://www.cdt.org/privacy/guide/protect/laws.php

CDT – privacy and apps
http://www.cdt.org/ask-mobile-apps-privacy

FCC: Bureau of Consumer Protection
http://business.ftc.gov/privacy-and-security

Council of Better Business Bureaus – collection of federal privacy laws
http://www.bbbonline.org/understandingprivacy/library/fed_stateprivlaws.pdf

National Conference of State Legislatures
http://www.ncsl.org/default.aspx?tabid=13463