De-Bugging Legal Issues in Bug Bounty Programs and VDP

P2P3-R03: De-Bugging Legal Issues in Bug Bounty Programs and VDP

Peter Fisk, Attorney, Lane Powell PC

De-Bugging Legal Issues in Bug Bounty Programs and VDP

Vulnerability disclosure is a hot topic, showing up in a number of keynotes and other sessions during this year's RSA Conference. In this peer-to-peer session, a small group with a range of experiences got together to discuss ways to better address the legal side of bug bounty and vulnerability disclosure programs. As an attorney working in privacy and data security, my main aim for this session was to improve the conversations between security teams and legal teams. We focused not on whether to have a program, but rather on legal issues to address in setting up and running a program. Of course every legal situation is unique and nothing here is legal advice, but we discussed a number of issues where the law and the practices of vulnerability disclosure intersect.

Bug Bounty Policy, Bug Bounty Contract

Even though bug bounty programs are becoming more widely accepted – one could say popular – the teams that set them up in organizations are still contending with concerns about external security researchers "going rogue" to exploit vulnerabilities. While there is no way to eliminate that risk, it's a risk that exists outside of whether an organization has a bug bounty program. Researchers who want to avail themselves of a published bug bounty program usually want to follow the rules.

As for setting rules, the program owner sets the terms for its program when it publishes a bug bounty policy (sometimes called the "program brief"). Although usually not labeled as such, in almost all instances a bug bounty policy is a contract, and it makes sense to think of it as one. In legal terminology, it is a unilateral contract – one side sets the terms of the contract, and the other side accepts the contract by performing under it.

If it's your program, then you set the terms for what research you want conducted and what activity is in and out of bounds. One way this happens is setting the scope of targets in the policy. Scope-setting should be done in collaboration with technical teams – don't let the lawyers handle the scope alone. Bug bounty policies can set limits in other ways too, like limits on public disclosure of vulnerabilities. On the other hand, the one-sided nature of these policies creates a take-it-or-leave-it situation for researchers, so the organization setting up a bug bounty program needs to consider what balance of incentives is likely to lead to useful research activity and vulnerability reports while maintaining the organization's comfort level.

Safe Harbor as Consideration

There has been a push in the community to make safe harbor clauses a standard part of all bug bounty and vulnerability disclosure policies. The issue is that independent security researchers operate at peril of civil and criminal legal claims for their activity in other people's systems. In a safe harbor clause the organization hosting a program commits not to pursue legal action against security researchers who comply with the bug bounty or vulnerability disclosure policy and submit reports. This allows the researcher to operate with an assurance of safety from legal action.

We also discussed different ways of phrasing safe harbor clauses. In some policies the program owners say that they "will not" or "promise not to" pursue legal action. Other policies state that the researcher "is authorized" to conduct security research as long as it is in line with the policy. Some add a promise from the program owner to tell third parties that the researcher's activity was authorized. We also discussed how some policies explicitly extend the safe harbor to cover research activity that accidentally goes outside the scope set in the policy.

Going back to the point of the bug bounty policy as contract, in the United States a contract needs "consideration" to be valid. The concept is that both sides have to exchange something of some value in order for a contract to be binding. In general a promise is enough, and a promise ***not*** to do something is just as good. For that reason, the promise not to pursue legal action contained in a safe harbor clause is likely to be sufficient consideration to make a binding contract. So while fairness to security researchers is a good reason to include a safe harbor clause in a policy, these clauses can be valuable to the program owner too, by bolstering enforceability of the contract.

Personal Information – A Sticky Issue

Customer personal information is one of the most important assets that organizations protect. If there is a vulnerability that allows outside parties to access customer information, then an organization would probably want to know about that vulnerability. But if an external security researcher succeeds in accessing a system that holds customer information, especially sensitive personal information, this could trigger customer notice duties under data breach notice statutes in effect in all U.S. states. Most organizations prefer not to hit that trigger if they can avoid it.

We talked about some approaches to this problem. One is to remove customer information from the scope of research allowed under the program. Another is to require researchers never to download any information, so there is no acquisition of personal information. We also talked about how a safe harbor clause that makes researchers "authorized" to perform security research might support an argument that there was no "unauthorized access" to personal information (a trigger in many states) – but there are risks in that approach. Another approach is to run a private or closed bug bounty program, strengthening the argument that a specified set of security researchers is "authorized."

Ultimately each organization has to decide its approach to personal information exposure in vulnerability disclosure programs based on the information assets it is protecting, the business, its risk posture, and any number of other factors. Organizations should be prepared for the possibility that they will have to notify individuals of data exposure. This is a question where legal counsel typically should be involved. The personal information exposure issues are similar under the GDPR and other sources of law, although the analysis and countermeasures may differ.

Legal Documents in a Bug Bounty or Vulnerability Disclosure Program

We talked about the toolkit of documents involved in running a bug bounty or vulnerability disclosure program:

1) **The bug bounty (or VDP) policy**, aka program brief. This sets the terms of the program, as discussed above.

2) **A good all-purpose non-disclosure agreement**. When research goes out of scope or something unexpected happens, an organization may need to ask a researcher to sign an NDA as a first step to minimize risk. It's better to draft it before it's needed. On the other hand, one session participant had a story of an unsolicited bug report from an external researcher, where the researcher refused to sign an NDA. Nonetheless, the researcher worked constructively with the organization to resolve the vulnerability. So a refusal to sign an NDA is not necessarily cause for immediate panic. (We also discussed how communications from researchers that lack finesse sometimes can sound threatening, but typically just reflect language challenges.)

3) **Other contracts outside the bug bounty program**. An organization running any kind of vulnerability disclosure program will want to review its other contract terms to make sure that the organization is being consistent in its security commitments. This includes contracts with B2B customers, vendors, and service providers. Similarly, customer Terms of Use and End User License Agreements may need review, and it may be worth adding some disclosure about the use of external security researchers. On this point, one participant noted that a household name B2B customer had asked whether his company runs a vulnerability disclosure program, because they saw it as a sign of overall security maturity.

Wrapping it up

Those are some of the major points from our discussion. The P2P format is an effective format for sharing wisdom throughout a group. Vulnerability disclosure is an area that keeps growing and evolving as we speak, so it was great to hear a range of perspectives and I look forward to seeing how the community keeps getting better in this area.