The Social Implications of Internet Anonymity

Description: To create some background for next week's discussion about the significant technical challenges involved in creating true anonymity on the Internet, this week Steve and Leo discuss the consequences of use and abuse of the extreme power afforded by many different forms of Internet anonymity, privacy, and freedom of speech.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-069.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-069-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 69 for December 7, 2006: Internet Anonymity, Part 1.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Dell. For this week's specials, visit TWiT.tv/dell.

Well, after that marathon edition last week of Security Now!, a whole, what was it, almost an hour and a half...

Steve Gibson: Actually it was more than that, it was 97 minutes.

Leo: I'm exhausted. But, you know, I should say Steve Gibson is here, and he's our security guru. And people loved it.

Steve: They really did. I got some positive feedback in our Security Now! newsgroup at GRC from people saying, I mean, I had one comment, someone said they thought it might have been the best Security Now! ever. And they liked the fact that we took our time, we thoroughly covered the topics. I think more by coincidence than anything else we had a really good selection of questions, you know, they were complimenting me on the questions. But it's like, well, I didn't really do anything different this time than I have before. I just read through a bunch of questions and found good ones. But I guess we just hit the sweet spot somehow.

Leo: I like the Q&As because of the variety. It's not just one topic. And often the questions – and I think this was the case last time – are ones that I myself go, hmm, I wonder. And so it's good. That's why I do call-in talk shows and call-in TV shows, because I think people ask the questions. Sometimes we as experts don't always ask the right questions. We know too much, maybe.

Steve: And of course doing that really keeps you on your toes, too', because as I listen to you on KFI I'm thinking, my God, this guy knows so much. No, really.

Leo: I fake it well.

Steve: The breadth of your knowledge is phenomenal.

Leo: It is, it's good training for that. I'm probably leaving that KFI show at the end of the month because I've been working seven days a week for three years, and it's finally taken its toll. My hair is falling out.

Steve: Your family's forgot – well, I think that...

Leo: Family? What family?

Steve: The birthday you may have recently had might be responsible for some of that hair loss, too, Leo.

Leo: And it's hard to choose any one of the many projects I have to let go. But because the radio show consumes both Saturday and Sunday, it really eats my weekends. I think that's probably the one that's going to go. And that's the thing, you know what, that's the thing that will suffer is that forced training every week on 20 or 30 topics is great. It keeps my mind going. If I seem dumber next year, you'll know why.

So this week we're going to talk about something I think is very important: Internet anonymity.

Steve: There's been a lot of interest from people posting their own questions on the Security Now! page at GRC. For example, people want to have a presentation about this network called TOR, which stands for The Onion Router, which is an anonymity-enhancing network. And so I've begun to do a lot of research onto the specifics of that so we could talk about it.

But in getting involved in this, I realized that there's a social issue, like a moral and ethical issue that sort of comes up when you talk about, well, when you talk about any powerful technology. And the Internet and the anonymity that it provides is a powerful technology. Famously, Einstein was very concerned about the uses to which his contribution to the development of the atom bomb would be put. And I think, as I remember, later in life he became really sort of a peace nut, really worried that this armament he had created was so powerful and so potentially susceptible to misuse and abuse that he partially regretted his role in that.

Leo: It's always a mixed bag. I think if you accept the notion that there are times when anonymity is important, if you're a whistle-blower, if you are in a repressive regime and you need to fight against it, there are lots of reasons that anonymity would be important. I've had this conversation with Phil Zimmerman, the guy who created PGP, and that's what he says. He says, unfortunately you don't get to choose. You either allow anonymity or not. And there are pluses and minuses to both, I guess.

Steve: Well, for example, it's certainly arguable that you cannot have free speech without anonymity. Because people will simply be...

Leo: Intimidated.

Steve: They will be less – yes, intimated, exactly, and less willing to speak freely if they know that there are consequences to what they could say. I have to say, Leo, I have been self-conscious sending some political email, like post 9/11, knowing that the United States government has become much more aggressive about scanning email. When I use hot terms and keywords and things, I find myself thinking, literally, my behavior is modified because I don't want a false-positive. I'm no terrorist. I'm a patriot and all that. But still it's just like you just get a little twitchy when you think that what you're saying could be triggering some automated system somewhere.

Leo: That's why I use PGP. One of these days we're going to get you using it because that's the point. But it also raises the specter of terrorists themselves using encryption.

Steve: Well, yes. And in fact, you know, sort of on the issue of the benefit of it, GRC maintains newsgroups. And we don't require anyone to authenticate themselves in any way. So most of the people there use handles, typical Internet handles, some random combination of words and letters and things that identify them. And that's the only way they're identified.

Now, we implemented the technology to essentially create a hash of their log-in, which is not in any way associated to their name or any other information, but it's a unique token which cannot be spoofed. And so the idea is that posters at GRC have a handle which is anonymous, but they also have a tag which every posting they make is stamped with that tag, which is just – it's literally – it's the result of a cryptographic hash. And what it means is that nobody is able to impersonate somebody else, even though everyone is able to remain anonymous.

And actually the other cool thing is that this allows people to securely delete their own postings if something happens and they regret what they posted, they were upset at the time. It's been a traditional problem with newsgroups is that you either could not delete, or anyone could delete, in which case you have specious deleters who are deleting other people's postings. So we didn't want that. But we also wanted people to be able to amend their own postings. And so this allows them to do that. But the point is that I'm really an advocate of allowing people to be anonymous if that's what they want because I think it gets the truth. I really think people feel much more free to say what they really think if they're anonymous.

Now, even in my own little microcosm, speaking about this just for a minute, there has been a downside to that. Back when I was being very vocal about raw sockets on Windows XP and created a huge furor in the industry, the newsgroups drew a lot of attention from what you could only call trolls, I mean, people who were trolling the group...

Leo: Awful, yeah.

Steve: It was really awful. Now, I refused to delete those postings. I have, you know, it's my server, my bandwidth, and my storage. And people there were saying, Steve, why are you allowing these people to badmouth you like this and just leave this content on the server? And my feeling was, well, that's their opinion. And who am I to say that they don't have as much right to post something negative about Steve Gibson and GRC as somebody else has to post something positive. I ended up being vindicated in that issue with Microsoft and raw sockets, which are now removed from XP after Service Pack 2. But it was a rough time. And it was about me sticking to the principle that people could post whatever they wanted to and do so anonymously. Arguably, if these people had to be identified, then they would probably not have posted that way. One of the things that we see on the Internet is much more outrageous behavior than you normally see in the physical world, where people are inherently more accountable for their actions.

Leo: Oh, yeah, BuggyBear2937 is very easily annoyed. And lets us all know it. I'm making that up, of course.

Steve: Oh, of course.

Leo: But that's the real problem is that it doesn't feel like a face-to-face. You are somewhat anonymous. And on sites where people use real names, you don't see that kind of problem. It's just tough because there are pros and cons to both sides.

Steve: I have to say, too, that if somebody uses an anonymous handle over time, and we have the ability to prevent that from being spoofed, as we do, what ends up developing over time is a trust in that person.

Leo: That's true, that's true.

Steve: I mean, that is, in that anonymous handle. That is, I'll never know who many of the valued contributors on our newsgroups are.

Leo: But they have identity. They've built an identity, even though it doesn't match their real name.

Steve: Exactly.

Leo: Now, and that's why – and maybe this is the answer. That's why a lot of message boards have an Ignore feature. So if, conversely, somebody proves their identity to be a complete butthead, you just press the Ignore button, and you don't see their stuff anymore. Maybe that's the kind of solution we need. Instead of saying, no, you've got to use your real name, we need maybe to do it some other way, more innovatively.

Steve: And of course in the press there's this whole notion – and even in law enforcement there is this notion of an anonymous informant. The famous Deep Throat, who was

participating in the whole Watergate issue and informing Bob Woodward of what was going on. This was a person who over time built up a relationship with this person in the press and so – and the same thing, of course, happens in law enforcement where somebody will have a confidential informant that over time has proven their integrity, may always need for whatever reason to remain anonymous, but feels that by providing certain information, more better is being done than harm. And that's sort of the way that decision gets made.

So the other thing that's interesting is, for example, there's a network called Freenet which is really a perfect example of very powerful technology where you're taking the good with the bad. Freenet allows the creation of private encrypted networks for storage of content. Now, that's something very different, for example, than other anonymizing services like the famous Anonymizer.com that's been around for a decade. They will allow you to anonymously acquire information, that is, for example, anonymously surfing the Internet so that you go to sites that have no idea who you are.

Now, as we're going to discuss next week, it turns out that unless this is done with much greater care than most people assume, that level of anonymity can be penetrated. So it turns out that really true anonymity on the 'Net is much harder to get than is normally believed. But Freenet is a different approach. They're very pro anonymity, pro privacy, pro free speech. So their system basically allocates a chunk of hard drive space from everyone participating in the network. And the content of Freenet is encrypted and stored in this big distributed database made up of all these different computers. Well, it's valuable certainly for people to be able to post and share their own content. Whereas, for example, as I said, with Anonymizer you're only browsing websites, and they specifically don't allow you to create content. In Freenet you can.

But it does mean that, as a participant in this network, you have no idea how your hard drive is being used. It could literally be, sure, it could be uplifting free speech articles about what's really going on with a government or actions somewhere in the world. But at the same time it could be really distasteful child pornography or something. And the point is, you are enabling that to be stored on your computer by availing yourself of this system. So it's a real mixed bag.

And the other issue is one of copyright. And it's interesting how copyright comes into this because the enforcement of copyright, that is, the actual enforcement of it, requires monitoring communications. That's how copyright is enforced is you're monitoring communication. But free speech, as we have said, cannot be guaranteed in an environment where there is monitored communications. So just logically that demonstrates that you cannot simultaneously have both freedom of speech and the enforcement of copyright.

Leo: You're right. QED, QED.

Steve: Exactly. And so many people have said, well, what if Freenet is used for sharing of copyrighted movies and files and music and content? And it's like, well, yes, that's a violation of copyright law. And so it's against the law for the system to be used in that way. But a system which robustly enforces freedom of speech – and we've already seen that freedom of speech requires anonymity, otherwise speech is really not unencumbered and not free, so you're going to have anonymity. And inherently that means that the anonymity creates free speech, and free speech means that copyright cannot be enforced.

So I guess the real point I wanted to make was that we're talking about potentially very powerful technologies which can be abused. As you were saying earlier, Leo, there is, for example, an issue with terrorists using networks like this to securely communicate among themselves. It's absolutely possible.

Leo: Of course when you're just encrypting the email, you can still tell who's sending a

message to whom; right?

Steve: So, for example, with PGP there is the knowledge that we've got endpoints that are communicating. And one of the differences with a system like Freenet, which is a rich network of interconnected systems which are encrypted, is that there isn't any way to demonstrate a point-to-point connection. Data can be deposited in this distributed, shared database, and it can be retrieved.

Leo: So if I use PGP to encrypt email to you, everybody knows, who's snooping on us, anyway, that you and I are having a conversation.

Steve: Exactly.

Leo: If I were to do it over Freenet, nobody'd know who I was talking to.

Steve: Exactly. And in fact, Freenet, I think it's currently at 0.7 is the current release. They have just added some technology to allow standard Internet-style bulletin board communications where people are able to have threaded discussions with complete assured anonymity and an inherent database, which is what any kind of a discussion board requires, and absolute encryption, and no ability to trace who sees what.

Leo: Do you want to talk a little bit about how Freenet works?

Steve: I'm going to get into the technology of this stuff next week because it is complicated. It turns out that, for example, Anonymizer, that is basically essentially just a proxy, Anonymizer is – well, any simple anonymizing proxy has the problem that, if communications is monitored upstream and downstream of it, that is, on either side of it, it's possible to associate the traffic pattern coming and going and determine the IP of someone visiting a given website. And that's something that people don't typically appreciate, the idea being that packet sizes vary, packet timing varies. And so if somebody – for example, the government – had the ability of monitoring the network traffic to and from Anonymizer, they would be able to see packets coming into Anonymizer and leaving, and basically penetrate that anonymizing proxy effect because the traffic would allow them to associate connections through the proxy and basically punch a hole in the entire thing.

So it turns out that obtaining this level of real anonymity is substantially more difficult than most people assume. It's just not a matter of running through a proxy which is going to reissue your HTTP communications from its IP rather than from yours. In fact, the TOR project says TOR only minimally hides such correlations between incoming and outgoing traffic. It says even TOR, which is a multi-hop, multilayered system, it says an attacker watching patterns of traffic at the initiator and at the responder will be able to confirm the correspondence with high probability.

Leo: The correspondence between you and me, let's say.

Steve: Well, yes, for example, if we were connecting through there. But normally TOR is used for robust anonymous surfing. It turns out, though, that it is not that robust.

Leo: Ain't so anonymous either, apparently.

Steve: Exactly. And that's the problem is they had to – and they deliberately, I mean, they understand the problem. The only way to really enhance this is to introduce much greater latency, that is, for the routers in the TOR network to hold the packets for a long period of time and then release them. Well, now, this is the kind of thing that you could do, for example, if you wanted to anonymously download files, where you're not trying to do real-time activities. But things like VoIP obviously require real-time responses. And to practically surf the web, to go from website to website clicking on links and downloading content, there's a tremendous amount of real-time interaction between your browser and the remote server as all of the various components of a web page are assembled.

So this notion of real-time anonymity turns out to be specious. It is almost impossible to get that. One way you can is if the anonymizer also is a big cache. Because if it's caching, then many of the things you need, the assets and resources and even the pages you go to, may already be in the cache. For example, people who use Google are probably aware that sometimes you'll click on a link in Google that is a link that Google has returned as a result of a search. And the site'll be down or offline or really slow, and you go okay, so you hit Stop on your browser, and instead you use Google's cached copy. So in that scenario you're never making your request outside of Google. It's going to Google, and you're taking advantage of Google's massive cache of the entire Internet in order to prevent actually going out to that server and getting the content. So there's an example where no one could detect, if they weren't looking inside Google, no one could detect from the outside, over for example an HTTPS, an SSL-secured connection to Google's cache, what it was you were looking at because Google would be the central repository of all these external sites. But that's exactly analogous to what Freenet does because Freenet creates this encrypted, secured database of discussion groups and massive amounts of content which is completely opaque from the outside. And due to the way it's set up, no one is able to determine what it is you're putting into this database and what it is you're pulling out.

Leo: So we don't want to get into details on how this works.

Steve: I want to do that next week because it's really interesting what the TOR guys did in order to create really robust security with their network.

Leo: So there's Freenet, there's TOR, and then of course there's local encryption, which doesn't eliminate the locale of where it's coming from or where it's going, but at least encrypts the content, like PGP or the new privacy guard, GPG, which I use.

Steve: Right. And I'm glad you brought that up because the point is, what's significant about that is that it's not anonymous.

Leo: Right. In the sense that you know who it is, yes, right.

Steve: Exactly. The content may be opaque and securely encrypted, but there's no anonymity provided by the people who are communicating at the endpoints. And very often that's something that people really need or want for various purposes. And again, the problem is there are many, many good reasons and beneficial reasons for having and enforcing and allowing anonymity on the 'Net. The flipside is, as with any really powerful technology, it can be used for nefarious purposes, as well.

Leo: There were for many years, and I don't know if they're still around, anonymous remailers, where you would use kind of – similar to a TOR or Anonymizer. You'd use multiproxies, and it would eventually hide who sent the email and where it was going. Unfortunately, I have to say, at least some of these have been subpoenaed by governmental agencies, and I guess it wasn't hidden enough.

Steve: Yes, in fact there was a case there, something called the Java Anonymous Proxy Project, which spreads anonymous proxies around the globe. It turns out that the state of Germany did not want these anonymous proxies functioning within their domain, literally, I mean their dominion, and generated legal action against these anonymizers. They legally required that a backdoor be installed in order for them to have access to what was going on. I mean, this kind of anonymity makes governments very uncomfortable.

Leo: And others, like the Church of Scientology, who compromised the Penet mailer. It's a fascinating subject. And we've just started, basically, as you have in the past, with kind of a roundup of the high-level issues. We'll talk about the technologies in the next episodes.

Steve: You know, we could have ignored the whole question of the value and benefit and importance and responsibility that comes with anonymity on the Internet because it's very significant because the Internet is such a powerful opportunity for giving people the freedom of speech and freedom of anonymity. But with that comes some responsibility. And there's a dark side, which I didn't want to not talk about that.

Leo: You can't ignore it. Although I am certainly a believer ultimately in free speech, and I think you've got to do it, despite the negatives, the downside. The alternative of completely no anonymity at all is just far worse.

Steve: And it seems to be – I don't mean to impose democratic politics on the world. Certainly the...

Leo: Lowercase "d," by the way, not uppercase "D" when you say "democratic."

Steve: Right, exactly, lowercase "d." Certainly the rulers of China have a different philosophy about the way they think a state should operate. But to the degree that a democracy is a valuable thing for people to have, we understand that that requires that the citizens of the democracy be informed of what the government is doing and that there be good communications in order for this state to be managed. And governments have historically fought that kind of really good communication. Governments would like to have more control. And it's the lack of control that makes the system work in the long term.

Leo: Steve, as usual, sometimes technology verges on politics. And this is a case where it does, and I think you've done a great job of synopsizing both sides. Next week the ins and outs, the technology behind Freenet and...

Steve: And why anonymity, why and exactly how technically obtaining real anonymity is a much more difficult thing to do on the 'Net than most people are aware.

Leo: It's hard to do. Thank you, Steve Gibson. Of course we want to remind everybody that Steve's site is the home, not only to this podcast, GRC.com, and the 16KB versions and the transcripts, but also to SpinRite, which is his daily bread. And if you ever have trouble with your hard drive, there's no question at all, SpinRite is a must. It's in my kit. When I go around and work on people's computers, it's one of the first programs I'll run. It's the ultimate disk recovery and maintenance utility, and it's highly recommended.

Steve: I got a neat piece of mail from someone who recently purchased a Dell Latitude notebook. He said: I purchased a brand new Dell Latitude notebook a couple of weeks ago and was very happy with the core duo, gig of RAM machine. He said: It started to boot really slowly, and programs would crash every so often. So I ran SpinRite, and what do you know, it started finding problems about halfway through the scan. So I emailed Dell and told them that SpinRite was used on the drive, and that I would require a new one. With no questions asked, they sent out a brand new hard drive the next day with prepaid return shipping.

Leo: That's great. That's great.

Steve: He said: The respect from Dell to the SpinRite product was phenomenal. They didn't even want me to run any other software to confirm the diagnosis.

Leo: They do.

Steve: He said: Thanks, Steve, you saved a brand new Dell from an untimely death.

Leo: Isn't that great.

Steve: That was really neat. And of course, you know, Dell can't control how the UPS driver may have been drop-kicking this guy's poor laptop...

Leo: Well, don't even blame UPS. Sometimes the hard drives just come out of the factory bad.

Steve: Exactly. It could pass initial tests and just have an infant mortality problem. But this guy ran SpinRite, it confirmed a problem, and Dell said, okay, that's all we need to know.

Leo: I love it. That's kind of a joint plug, really, for SpinRite and our sponsor. I like it. Very nicely done.

Steve: True story.

Leo: I actually just bought a Dell laptop, an M1210, which is a dual core 2 with two gigs of RAM. I loaded this sucker up. Actually I was amazed because the price for really absolute top-of-the-line laptop was about $2,000. And that's so much less than it used to be. In fact, we used to say the computer you want is always at least $2,500, and the dream

computer's like 3 or $4,000.

Steve: It was always a moving target.

Leo: Yeah. Core 2 duo, 2GHz processors, two gigs of RAM. I got a 7200 RPM hard drive because I wanted to – this is going to be my Vista machine, so I really wanted to trick it out, knowing that Vista is going to be demanding. They don't have hybrid hard drives yet, unfortunately. But everything else, I just loaded that sucker up. I was very pleased. If you want a link to that or to other Leo's Picks, including the XPS that we bought for Call For Help, that you'll find at TWiT.tv/dell. That's the Leo's Picks page. Dell does provide us with financial support for this podcast and a number of the other TWiT podcasts. They've been a really great sponsor. In fact, I think our contract runs out in the next couple of weeks, and I'm hoping that we can get them to come back. But I do appreciate their support, and your support, too. When you buy any Dell product by going through one of the links on the TWiT.tv/dell page, we get credit for it. And so thanks to Dell for their support.

Oh, also want to mention Astaro because they have been here since practically day one. I can't remember exactly what episode they joined us on, but early on. They've been big supporters of the show.

Steve: And they were our first sponsor.

Leo: They were our first sponsor. They were the first sponsor on the TWiT network. And they've decided to come back for another year. And that's – we love them. And there's good reason. It's an open-source, high-quality security gateway. If you have a small or medium business, and you need superior protection from spam, from viruses, from hackers, you get a complete VPN, intrusion protection, content filtering, and of course an industry-strength firewall, all in a very easy to use, high-performance appliance. I've got one, and I just love it. It's the Astaro Security Gateway. Contact them, they'll give you a free trial – www.astaro.com, or call 877-4AS-TARO. You can schedule a free trial. And home users, non-business users, can download the software version of ASG free for home use also. Astaro.com. Thanks to them.

Steve: So next week is talking about the technical challenges of Internet anonymity. I did mention last week that I would have a new piece of security-oriented freeware to announce. Unfortunately, we're recording this and next episode early.

Leo: Ahead of time, yeah.

Steve: Yes. And I've got myself tangled up in some tricky details with it. It's going to end up being, I think, even cooler and more valuable than I originally expected; but it's also turning out to be a lot more challenging. So I'm going to delay the announcement until I actually have the thing running and bulletproof and tested. So it'll be a couple weeks, and then we'll talk about what that is.

Leo: No problem at all. You're in heaven, though, aren't you, when you get to code on a new project.

Steve: Oh, finally, Leo, I'm back to writing some code.

Leo: Does that make you feel good? That's neat, I can tell. Are you running this in Assembly?

Steve: Of course.

Leo: Oh, Steve. You're so old-fashioned.

Steve: That's my language.

Leo: I love it.

Steve: Well, it turns out that it's exactly the right language for this application because I'm dealing with, down in the registers of Intel processors, dealing with literally setting bits on and off and protected mode and privileged instructions and that kind of stuff. So it's a...

Leo: Will this work on Vista as well as XP?

Steve: Yes.

Leo: Really. How do you know that? Did you test it in Vista?

Steve: Yeah. I've got it running on Vista. In fact, I have a new MacBook with the Intel core 2 duo because I needed some more recent chips in order to see it running there. And Leo, I've got to tell you, I'm going to disabuse you of this notion that Vista requires a lot of power. I am really happily running it on my little HP TC1100 notebook, I mean, my little...

Leo: That thing is low power. That's the old tablet, yeah, that's not very fancy. I mean, that's Pentium M, right?

Steve: Yes. The 1000 was a Transmeta, and they realized, whoops, that was a mistake. And so they went to the 1100, which is a Pentium M, I think it's 1.2GHz or something. But it is completely usable.

Leo: That's good news.

Steve: And I'll tell you, I don't have the – my God, I'm never going to remember the name of this UI. The Glass? Is it Glass?

Leo: Aero Glass.

Steve: Aero Glass. I don't have that, but...

Leo: You don't need that.

Steve: I really don't need it. And Leo, there are so many little touches. There's now stroke recognition on the tablet. So you're able to scroll a browser page just by stroking up or down. You're able to copy, paste, cut, and delete using stylus strokes. Anyway, I'm seriously considering maybe just skipping over XP and going to Vista because I really think this is...

Leo: I think you should.

Steve: You and Paul were talking on Windows Weekly on Friday, saying that in his opinion, because he's of course been really exposed to it, he thinks it's like Microsoft really got it right.

Leo: I'm excited about it. I'm totally excited about it.

Steve: And here I am saying – Mr. Skeptic, Mr. Oh Don't Touch It for a Couple Years, blah blah blah. It's like, well, there's a lot to like about it.

Leo: In fact, I have to say, on this M1210, it's running XP because I haven't yet got my MSDN subscription. And I don't – it's like I don't even want to try it. I know XP. I'm not interested. I want Vista. I want Vista. And I'm sure everybody else is saying the same thing.

All right, well, we're just going to say good bye, and see you next week. And thank you, Steve. All right. And we'll see you all back here, same time, same place, for Security Now!.