OBAMA'S LEGAL HACKS

I have a piece over at The Week on the unusually credible denial the government issued on Friday, claiming they did not know of the Heartbleed vulnerability until earlier this month. In it, I note that Obama adopted a much lower bar for using software vulnerability than his hand-picked Review Group recommended in December. Most troubling, Obama admits he will use exploits for law enforcement, in addition to national security.

> But the announcement's discussion of the interagency review also made clear that the process will, sometimes, approve such a use — which means that the next Heartbleed could be exploited by the NSA. Furthermore, the standard the administration claims to have adopted — "a clear national security or *law enforcement* need" (italics mine) — is lower than the "urgent and significant national security priority" recommended by the Review Group.
>
> In other words, in very clear language, the government has confessed that it does and will continue to keep secret Heartbleed-style vulnerabilities not just for national security purposes, but also for mere law enforcement.

The idea that the government might hack in the name of law enforcement is not new.

As WSJ reported last month, DOJ is trying to get the Judicial Conference to approve language allowing it to get warrants to hack in multiple districts at once.

> The government's push for rule changes sheds light on law enforcement's use of remote hacking techniques, which are being deployed more frequently but have been protected behind a veil of secrecy for years.

> In documents submitted by the government to the judicial system's rule-making body this year, the government discussed using software to find suspected child pornographers who visited a U.S. site and concealed their identity using a strong anonymization tool called Tor.
>
> The government's hacking tools—such as sending an email embedded with code that installs spying software — resemble those used by criminal hackers. The government doesn't describe these methods as hacking, preferring instead to use terms like "remote access" and "network investigative techniques."
>
> Right now, investigators who want to search property, including computers, generally need to get a warrant from a judge in the district where the property is located, according to federal court rules.
>
> In a computer investigation, that might not be possible, because criminals can hide behind anonymizing technologies. In cases involving botnets—groups of hijacked computers—investigators might also want to search many machines at once without getting that many warrants.
>
> Some judges have already granted warrants in cases when authorities don't know where the machine is. But at least one judge has denied an application in part because of the current rules. The department also wants warrants to be allowed for multiple computers at the same time, as well as for searches of many related storage, email and social media accounts at once, as long as those accounts are accessed by the computer being searched.

I especially applaud the way WSJ highlighted

DOJ's complaints about Orin Kerr calling what they do hacking.

Even more timely, a team of computer security experts — Steve Bellovin, Matt Blaze, Sandy Clark, and Susan Landau — just published a paper arguing that legal hacking is a better means to conduct law enforcement collection than a CALEA-type solution. But they argue that the government can and must achieve this law enforcement objective without compromising the security of the network.

> ¶162 As we alluded to earlier, this is a clash of competing social goods between the security obtained by patching as quickly as possible and the security obtained by downloading the exploit to enable the wiretap to convict the criminal. Although there are no easy answers, we believe the answer is clear. In a world of great cybersecurity risk, where each day brings a new headline of the potential for attacks on critical infrastructure,239 where the Deputy Secretary of Defense says that thefts of intellectual property "may be the most significant cyberthreat that the United States will face over the long term,"240 public safety and national security are too critical to take risks and leave vulnerabilities unreported and unpatched. We believe that law enforcement should always err on the side of caution in deciding whether to refrain from informing a vendor of a vulnerability. Any policy short of full and immediate reporting is simply inadequate. "Report immediately" is the policy that any crime-prevention agency should have, even though such an approach will occasionally hamper an investigation.241
>
> ¶163 Note that a report immediately policy does not foreclose exploitation of the reported vulnerability by law

> enforcement. Vulnerabilities reported to vendors do not result in immediate patches; the time to patch varies with each vendor's patch release schedule (once per month, or once every six weeks is common), but, since vendors often delay patches,242 the lifetime of a vulnerability is often much longer. Research shows that the average lifetime of a zero-day exploit is 312 days.243 Furthermore, users frequently do not patch their systems promptly, even when critical updates are available.24
>
> ¶164 Immediate reporting to the vendor of vulnerabilities considered critical will result in a shortened lifetime for particular operationalized exploits, but it will not prevent the use of operationalized exploits. Instead, it will create a situation in which law enforcement is both performing criminal investigations using the wiretaps enabled through the exploits, and crime prevention through reporting the exploits to the vendor. This is clearly a win/win situation.
>
> [snip]
>
> ¶166 The tension between exploitation and reporting can be resolved if the government follows both paths, actively reporting and working to fix even those vulnerabilities that it uses to support wiretaps. As we noted, the reporting of vulnerabilities (to vendors and/or to the public) does not preclude exploiting them.247 Once a vulnerability is reported, there is always a lead time before a "patch" can be engineered, and a further lead time before this patch is deployed to and installed by future wiretap targets. Because there is an effectively infinite supply of vulnerabilities in software platforms,248 provided new

> vulnerabilities are found at a rate that exceeds the rate at which they are repaired, reporting vulnerabilities need not compromise the government's ability to conduct exploits. By always reporting, the government investigative mission is not placed in conflict with its crime prevention mission. In fact, such a policy has the almost paradoxical affect that the more active the law enforcement exploitation activity becomes, the more zero-day vulnerabilities are reported to and repaired by vendors.

They go on to propose a legal regime that can provide clear guidance on which vulnerabilities should be reported, even analogizing the emergency period in which an agency can wiretap before getting a warrant.

But here's the thing: NSA's Bull Run program got reported in September, and since then the government has remained coy about whether it uses or even seeds vulnerabilities in software, even though anyone paying attention knew it does. It took claims that the government had been using the Heartbleed vulnerability for two years for the Administration to admit, tacitly, the earlier reports were correct.

The kind of legal regime Bellovin et al recommend requires that this law enforcement function operate within a legal — and therefore publicly acknowledged — framework, rather than piggy backing on the NSA's executive authorities in secret.

While Friday's admission is a start, and while it may be true that hacking presents a better solution to law enforcement needs than CALEA, these questions need to be openly discussed.

Otherwise, DOJ not only is hacking — in the dictionary definition Orin Kerr applied — but hacking in the reckless manner that DOJ prosecutes.