WANTED: SPECTRUM BOUNTY HUNTERS

WILSON SCARBEARY†

Politicians on both sides of the aisle love to promote market solutions to regulatory problems, especially when it comes to telecommunications policy. Despite this preference, bounties, and similar financial incentives—historically, popular market solutions to regulatory problems—have yet to be widely used in wireless policy. In response, this paper considers three hypothetical kinds of bounty programs that could be used to regulate harmful interference or address critical vulnerabilities in wireless systems. A number of legal barriers, market forces, and other considerations will likely limit the effectiveness of these programs in the near term, but bounties still offer tremendous promise for wireless regulation. As wireless technology becomes ubiquitous in our everyday lives, our wireless "ecosystem" is becoming increasingly congested. In this new crowded ecosystem, bounties may likely become an effective and efficient tool for wireless regulation.

† J.D., University of Colorado. I would like to sincerely thank Dale Hatfield for his mentorship and guidance on the entire project, and Aarjav Chuahan for his assistance in researching and drafting the analysis of software bug bounties. Without their support, this paper would not have been possible. The inspiration for this paper was first brought to Dale Hatfield's attention by Milo Medin, Vice President of Wireless Services at Google and a member of the FCC's Technological Advisory Council. Over the course of writing this paper, we consulted with a number of experts in wireless and telecommunications policy to solicit feedback on our proposals and identify key issues. We would like to thank all of our reviewers for taking the time to read our early drafts and provide valuable insights. While we relied on these reviewers for input and feedback, any errors in the final draft are our responsibility alone. Mark Bykowsky, Office of Economics and Analysis, Federal Communications Commission; Pierre de Vries, Co-Director of the Spectrum Policy Initiative, Silicon Flatirons Center; Rebecca Dorch, Senior Spectrum Policy Analyst, Institute for Telecommunication Sciences, National Telecommunications and Information Administration; Anna Gomez, Partner, Wiley Rein LLP; Keith Gremban, Former Director, Institute for Telecommunication Sciences, National Telecommunications and Information Administration; Research Professor, College of Engineering and Applied Sciences, University of Colorado Boulder; Bruce Jacobs, Senior Advisor, Office of Spectrum Management, National Telecommunication and Information Administration; Milo Medin, Vice President, Wireless Services, Google; Tom Power, Senior Vice President & General Counsel, CTIA; Blake Reid, Clinical Professor, Samuelson-Glusko Technology Law & Policy Clinic, University of Colorado Law School; Amie Stepanovich, Director, Silicon Flatirons Center, University of Colorado Boulder; Jane Thompson, Associate Director of Faculty Services and Research, University of Colorado Law School; Phil Weiser, Adjunct Faculty & Dean Emeritus of the University of Colorado Law School

INTRODUCTION

A bounty is a premium or benefit offered as an incentive to induce someone to take action or perform a service.[1] Bounties have traditionally been used to address both civil problems and aid in the enforcement of criminal laws. For example, a civil bounty might be given to a hunter for returning the carcass of a predator, where a criminal bounty might be given to an informant who aids in the prosecution of a criminal.[2] Bounty programs have also recently gained popularity as a tool to incentivize security research in both the private sector and the federal government.[3] Drawing inspiration from these traditional uses of bounty programs, we consider three hypothetical wireless bounty programs that could be used to address various goals in telecommunications policy and wireless regulation.

First, we consider whether whistleblower rewards could be an effective tool to aid the Federal Communications Commission ("FCC" or "Commission") in wireless enforcement. Individuals who bring information to the Commission's attention that leads

1. *Bounty*, BLACK'S LAW DICTIONARY (Bryan A. Garner ed., 11th ed., 2019).

2. *See* ELMER W. SHAW, AN ANALYSIS OF THE LAWS RELATED TO THE BOUNTY ON WOLVES IN THE UNITED STATES, 1,6 (Libr. Of Cong., Legis Reference Serv. 1970). (discussing the history of bounties for wolves); *see also* Marsha J. Ferzinger & Daniel G. Curell, *Snitching for Dollars*: *The Economics and Public Policy of Federal Civil Bounty Programs*, 1999 Univ. Ill. L. Rev. 1141 (1999) (discussing the use of whistleblower bounties by federal agencies).

3. *See generally* Huw Fryer & Elena Simperl, *Web Science Challenges in Researching Bug Bounties*, *in* PROC. 2017 ACM CONF. ON WEB SCI. CONF. 273, 273–77 (WebSci 2017), https://dl.acm.org/doi/pdf/10.1145/3091478.3091517?casa_token=t5xWD10pn0wAAAAA:r3FPxwAVrjzGavDRwFgUrueo3myZXb0ULnNm3Mu-6tWT__GbC33MEE4J4AVdYoEcFuVaVeCxWeit1A [https://perma.cc/K4X2-RMTS].

to the seizure of illegal equipment or issuance of fines could be offered a small cut of the government's proceeds. Assuming that the government actually receives the proceeds from these actions, whistleblower rewards could aid the Commission's enforcement efforts.

These kinds of incentives will be most effective where they are used to complement—not replace—existing enforcement efforts by the Commission. A whistleblower bounty program could allow the Commission to focus more of their limited resources on protecting public safety while supporting market solutions to interference that creates more private harms.

Second, we consider how buyback programs might be used as a tool for managing wireless devices. Device manufacturers might offer incentives for consumers to return old or malfunctioning devices to manage risk, prevent or reduce interference issues, or accelerate adoption of new technologies. The Commission might also use buyback programs to incentivize the collection of harmful devices or outdated technologies to manage spectrum or promote a better economic use thereof.

Buyback programs or product recalls are already a well-worn strategy for managing risk in private markets, but these kinds of programs have had fairly mixed results when run by the government.[4] Nonetheless, these programs have some promise as a method of managing an increasingly crowded spectral ecosystem where an exploding number—and variety—of devices compete for access. In particular, these kinds of programs may become critical to manage new modalities of spectrum allocation—like Citizens Broadband Radio Service (CBRS)—that blur the lines between licensed and unlicensed use and may call for new approaches to spectrum and device management.[5]

Third, we consider how bug bounties could be used to address wireless vulnerabilities. Bug bounty programs—which offer rewards to security researchers who discover and disclose security vulnerabilities—have become increasingly popular as a tool for promoting security and managing risk on software

4. *See generally* Atif Mian & Amir Sufi, *The Effects of Fiscal Stimulus: Evidence from the 2009 Cash for Clunkers Program*, 127 Q.J. ECON. 1107 (2012).

5. *3.5 GHz Band Overview*, FED. COMMC'N COMM'N (Mar. 10, 2020), https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview [https://perma.cc/N94C-8LFG].

platforms.[6] Despite the popularity of bug bounty programs in the software world, bug bounties are not currently widely used to identify and solve wireless vulnerabilities.[7] Wireless bug bounties might be used to identify vulnerabilities in private systems (such as autonomous vehicles) or in public safety systems (such as GPS.)

In either case, for wireless bug bounties to be successful, security researchers will need clarity from regulators regarding legal boundaries and other limitations on their work. In the world of software—where companies are welcoming of security research and some existing precedent defines the boundaries of acceptable conduct—there is at least some clarity for security researchers to conduct their work.[8] For wireless security research to be as effective, the Commission will need to clarify its approach to enforcement in order to encourage valuable research.

All of these hypothetical bounty programs have some promise, but also face several issues that will make implementation difficult. For the Commission to offer any of the discussed bounties, Congressional authorization is likely necessary. Further, even if authorization were to happen, the current financial incentives may not be sufficient to actually make bounties an effective tool for spectrum regulation. However, as wireless ecosystems become increasingly crowded—and critical to our everyday lives—the market may be able to offer better incentives.[9] With this more robust market, Congress

6. *See* Andrew Marino, *How the commercialization of bug bounties is creating more vulnerabilities*, THE VERGE (July 7, 2020, 1:55 PM), https://www.theverge.com/2020/7/7/21315870/cybersecurity-bug-bounties-commercialization-katie-moussouris-interview-vergecast-podcast [https://perma.cc/Z6C2-6897].

7. *See* Fryer & Simperl, *supra* note 3, at 274.

8. As an example of a friendly company, Apple has recently offered special handsets to security researchers in an effort to promote reporting of software vulnerabilities. *See* Oliver Haslam, *Apple is now supplying bug bounty hunters with special iPhones*, IMORE (July 22, 2020), https://www.imore.com/apple-now-supplying-bug-bounty-hunters-special-iphones [https://perma.cc/5MS6-ZUVJ].

9. Both the raw number of devices, and the sheer variety of wireless or internet-connected devices are steadily growing. *See* Dave Evans, THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING, CISCO 3 (2011), https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [https://perma.cc/MGM3-2ZGZ].

may be more inclined to pass legislation that creates the necessary legal framework for these programs to succeed.

I. CAN WHISTLEBLOWERS ADD VALUE TO FCC ENFORCEMENT?

Whistleblower bounties are currently used by agencies like the Securities and Exchange

Whistleblower bounties are currently used by agencies like the Securities and Exchange Commission (SEC) and Internal Revenue Service (IRS) to aid in the prosecution of crimes like insider trading or tax evasion.[10] These existing federal agency bounty regimes were created by Congressional authorization.[11] Assuming Congress structures the discussed bounty in the same way as existing federal whistleblower bounties, the Commission could offer a fixed cut of enforcement proceeds to individuals who bring information forward concerning interference or other statutory violations. Whistleblowers who come forward under this program might include:

(a) Ordinary citizens who are offered an opportunity to purchase illegal equipment while attempting to purchase legal equipment from a vendor;

(b) Industry insiders (such as device manufacturers or supply chain workers) that discover information concerning the illegal distribution of regulated devices, like jammers[12]; or

(c) Any person who provides information concerning ongoing malicious interference such as operation of a pirate radio station, continued use of radio frequency jamming devices, or other criminal acts under the purview of the FCC.

A threshold issue for any whistleblower program is that the government needs to actually receive monies from any corresponding enforcement action.[13] In addition, the information brought forward by the whistleblower also must have been essential in helping commence enforcement, usually by aiding in the establishment of guilt in a criminal proceeding.[14]

10. *See* Ferzinger & Curell, *supra* note 2, at 1144.

11. *See* Insider Trading and Securities Fraud Enforcement Act of 1988, 15 U.S.C.A. § 78u (2021) (creating the Bounty Program at the SEC).

12. *See infra* Section 4 (discussing various kinds of wireless attacks and technologies).

13. *See* Ferzinger & Curell, *supra* note 2, at 1147.

14. *Id.* at 1150.

Another consideration is that existing programs preclude government employees from receiving any kind of bounty.[15] The SEC program takes this a step further by prohibiting any individual currently under investigation from receiving a reward for turning on their co-conspirators.[16] By contrast, other federal agencies like the IRS leave open the possibility of conspirators to a crime receiving a reward for coming forward.[17]

Existing programs also cap rewards at a fixed percentage of whatever proceeds the government *recovers*. Some agencies go further by imposing a nominal cap on rewards. For example, the IRS offers informants up to a 15% of collected backed taxes, but imposes a nominal cap of $10,000,000.[18] By comparison, the SEC offers a 10-30% of the proceeds with no nominal cap on rewards.[19]

One reason for the relatively low reward percentages under existing bounty programs is the pressure for these programs to be revenue-positive for the enforcing agency.[20] Agencies can depend on the rewards from enforcement actions to fund administrative costs of the bounty program itself. In most cases, agencies use the proceeds from enforcement actions to fund other expenses.[21] However, when the government is successful in collecting monies, even a small percentage can be a significant incentive to come forward.[22]

Substantial rewards—or simply a desire to do the right thing—will motivate some to come forward, but most informants will consider a variety of factors when contemplating blowing the whistle on their coworkers or friends. From a pure economic standpoint, informants come forward when their discounted gains exceed their discounted losses.[23] In other words, informants will consider not only the relative sizes of the

15. *Id.* at 1147.
16. *Id.* at 1149.
17. *Id.* at 1148–49.
18. *Whistleblower Office*, INT'L REVENUE SERV., https://www.irs.gov/compliance/whistleblower-informant-award [https://perma.cc/B2J2-MYQ3] (last visited Sept. 26, 2021).
19. *Office of the Whistleblower*, SEC. & EXCH. COMM'N, https://www.sec.gov/whistleblower [https://perma.cc/X8RX-33S4] (last visited Sept. 26, 2021).
20. *See* Ferzinger & Curell, *supra* note 2, at 1156.
21. *Id.*
22. *Id.* at 1170.
23. *Id.* at 1171.

potential rewards or costs but also the likelihood of occurrence.[24] For example, if an informant stands a 25% chance of receiving a $1,000,000 reward, their discounted gains will equal $250,000. Similarly, an informant who stands a 40% chance of losing $500,000 as a result of coming forward would have a discounted loss of $200,000.

While this type of positive economics is an interesting academic tool, it is worth noting that the majority of informants likely do not engage in these types of mathematical calculations when deciding whether or not to come forward.[25] Nevertheless, these economic principles illuminate how whistleblower programs can be structured to encourage more participation. In particular, it highlights the importance of not just offering an enticing reward, but also a strong payout guarantee.

Unfortunately, a key takeaway from this model is that our hypothetical FCC bounty program is unlikely to succeed, at least in the status quo. Unlike the fines typically collected under other federal bounty programs, the Commission's fines are paltry. DOJ judgements under the False Claims Act and fines for insider trading can exceed $50,000,000.[26] By contrast, the FCC recently issued a fine over $450,000 for operation of a pirate radio station—the largest fine ever issued for such an offense.[27] Additionally, the Commission has a poor track record of actually *collecting* fines, especially where the offenders are foreign corporations or simply insolvent.[28] Both of these factors dull the potential effectiveness of a whistleblower bounty program in today's enforcement environment.

However, the winds may be shifting in favor of bounties as spectrum becomes an increasingly valuable part of not just our economy but also our national defense and homeland security. In fact, the Commission recently announced their largest fine ever—$2,800,000—against a drone manufacturer for marketing

24. *Id*. at 1171–72.

25. *Id*. at 1179.

26. *See id*. at 1170.

27. *FCC Proposes Fine of Over $450,00 Against Boston-Area Pirate Radio Operator*, FCC (Dec. 12, 2019), https://docs.fcc.gov/public/attachments/DOC-361345A1.pdf [https://perma.cc/9STV-3RBJ].

28. *See* Jon Brodkin, *FCC "fined" robocallers $208 million since 2015 but collected only $6,790*, ARS TECHNICA (Mar. 28, 2019, 3:17 PM), https://arstechnica.com/tech-policy/2019/03/fcc-fined-robocallers-208-million-since-2015-but-collected-only-6790/ [https://perma.cc/Y2RB-C9Y3].

transmitters that failed to comply with regulations.[29] The Commission specifically called out the public safety implications of interference as a justification for the issuance of such a large fine.[30] Fines of this size are beginning to approach the amount necessary to support a robust whistleblower program.

It is worth noting that our potential FCC whistleblower program might not need to remain revenue positive. Unlike the crimes targeted by existing programs—such as tax evasion or securities fraud—the conduct targeted by our hypothetical enforcement program could have dire public safety consequences. In this environment, Congress might decide that the public safety benefits justify more substantial rewards. Congress has certainly indicated that they take protecting systems like GPS seriously while pointing out the potential consequences of interference for the economy, public safety, and national defense.[31]

Nonetheless, a revenue positive whistleblower program would be significantly more likely to aid in the Commission's enforcement efforts. Assuming that the Commission can successfully *collect* the proceeds from enforcement actions, the revenue could be spent to expand enforcement efforts. This might include expanding enforcement to protect public safety systems, or helping manage and resolve disputes between private spectrum holders.

As spectrum becomes increasingly crowded and a more critical part of the public safety and national defense systems, interference management will only increase in importance. This shift will call for new approaches to wireless regulation and enforcement. Market-based solutions like a whistleblower bounty program could be a politically popular option. No doubt, some politicians may be morally opposed to the idea of paying people to do the FCC's "dirty work;" however, on balance, these programs are likely to receive bipartisan support.[32]

---

29. ABC Fulfillment Serv. LLC, 20 F.C.C. 101, 1–2 (2020), https://docs.fcc.gov/public/attachments/FCC-20-101A1.pdf [https://perma.cc/U5YT-R7VX].

30. *Id.*

31. *See* Jim Inhofe et al., *FCC and Ligado Are Undermining GPS - And With It, Our Economy and National Security,* U.S. SENATE COMM. ON ARMED SERV. (Apr. 22, 2020), https://www.armed-services.senate.gov/press-releases/inhofe-reed-smith-and-thornberry-in-defense-news-fcc-and-ligado-are-undermining-gps_-and-with-it-our-economy-and-national-security [https://perma.cc/T796-84WC].

32. *See* Ferzinger & Curell, *supra* note 2, at 1194.

Interference with these critical systems, like GPS, could justify issuance of large punitive fines—even a small percentage of which would be a significant motivation to incentivize whistleblowers. However, even without increased financial incentives, the public safety implications of harmful interference could motivate more whistleblowers to come forward simply out of a desire to protect others or do the right thing.

II. CAN DEVICE BUYBACKS HELP MANAGE AND PROTECT NETWORKS?

Bounties have long been used as an incentive for individuals to hunt predators or invasive species.[33] Wildlife bounties are still used today; however, recycling or bottle collection programs serve as a more ubiquitous modern example of bounty systems in action.[34] Similar buyback schemes have also been used as an incentive for individuals to adopt new technologies.[35] For instance, the "Cash for Clunkers" program gave rebates in an effort to encourage consumers to upgrade to newer, more efficient, and environmentally-friendly vehicles.[36] Despite some differences, all of these buyback programs seek to enable market solutions to problems such as pollution or environmental degradation. In every case, consumers are financially incentivized to help mitigate pollution or stimulate the economy by turning in their items.

Buyback programs like these could be used to facilitate market solutions to spectrum issues, including interference or

33. Shaw, *supra* note 2, at 6 (discussing the history of wolf bounties in the US); Dexter Thomas, *Louisiana is Paying $6 for Every Swamp Rodent You Can Kill*, VICE NEWS (Mar. 10, 2020), https://www.youtube.com/watch?v=AladRZv_pAo [https://perma.cc/LG22-5AFN] [(discussing a bounty program to contain an invasive species); *see also* Definition of Externality, INVESTOPEDIA (OCT. 26, 2020), https://www.investopedia.com/terms/e/externality.asp [https://perma.cc/3KG5-VX3N]
(an externality is a cost or benefit caused by a producer that is not financially incurred or received by that producer).

34. Finn Arne Jørgensen, *A Pocket History of Bottle Recycling*, THE ATL. (Feb. 27, 2013), https://www.theatlantic.com/technology/archive/2013/02/a-pocket-history-of-bottle-recycling/273575/ [https://perma.cc/7EV3-MLJH].

35. *See* Nick Bunkley, *Government Will End Clunker Program Early*, N.Y. TIMES (Aug. 20, 2009), https://www.nytimes.com/2009/08/21/business/21clunkers.html?_r=1&scp=3&sq=cash%20for%20clunkers&st=cse [https://perma.cc/Y9MF-HMAU].

36. *Id.*

inefficient use of spectrum. For example, device manufacturers might offer buyback payments—similar to bottle collection programs—to remove devices that have been shown to cause harmful interference or present other risks. The Commission could also incentivize parties to find and collect offending devices by offering to reduce fines based on the number of devices returned. Buyback programs might also be used to facilitate new methods of spectrum management or allocation. Lastly, buyback payments might be offered to clear devices from a particular band to mitigate interference issues or promote the adoption of new technologies.

In the 1950's, a new technology—disposable containers—brought about new economic opportunities but also a troubling new problem: excessive waste.[37] In response, environmental activists pushed for companies to share responsibility for this issue. Their efforts eventually convinced companies like Coca-Cola to offer incentives for customers to return bottles, encouraging recycling.[38] These payments allowed producers to save money on production costs while creating an incentive for consumers to engage in this mutually beneficial activity.[39]

While these kinds of buyback payments have not been greatly successful in the United States, these programs have been effective in other countries where larger incentives are offered.[40] For example, in Norway, the payments for each returned bottle significantly exceed those in the United States.[41] As a consequence, roughly 95% of beverage containers sold in Norway are recycled, and even wealthy Norwegians report turning in their bottles, not for the environmental impacts, but for the money.[42]

Much like the explosion of consumer waste in the 1950s, today's wireless devices are growing at an exponential rate.[43] The explosion of Internet-of-Things (IoT) devices has opened the door to a number of problems—and not just the growing issue of

37. Jørgensen, *supra* note 34.
38. *Id.*
39. *See id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. Evans, *supra* note 9, at 2–3.

electronic waste.[44] An exponentially growing number and variety of devices now compete for spectrum in an increasingly crowded ecosystem.[45] The natural consequence of this more crowded spectrum ecosystem is an increased potential for interference. The consequences of interference have also increased in our wireless world. Spectrum is critical for public safety systems, like GPS, and also assists in the operation of autonomous vehicles. Incidental interference with technologies like these could potentially prove fatal. The explosion of wireless devices only increases the potential for this interference.

For example, the Commission recently conducted enforcement proceedings against companies for operating devices that were unintentionally interfering with Terminal Doppler Weather Radar (TDWR), a critical public safety system.[46] In an increasingly crowded spectrum ecosystem, interference issues like this may become more common. Even where devices are being operated in accordance with FCC regulations and are properly configured, aggregate interference can *still* occur where devices are installed in a dense cluster.[47]

Beyond interference issues, the rise of IoT devices creates new, frightening security risks that could expose manufacturers to additional liability.[48] In all these cases, buyback bounties could serve as an effective tool for managing the potential risks.

Buyback programs might also be used to facilitate spectrum management by allowing for devices to be collected and replaced as a means of facilitating the adoption of new technologies or

---

44. Syed Faraz Ahmed, *The Global Cost of Electronic Waste*, THE ATL. (Sept. 29, 2016), https://www.theatlantic.com/technology/archive/2016/09/the-global-cost-of-electronic-waste/502019/ [https://perma.cc/ZCN7-3MGP].

45. Evans, *supra* note 9, at 9.

46. *U-NII and TDWR Interference Enforcement*, FCC (Aug. 26, 2019), https://www.fcc.gov/general/u-nii-and-tdwr-interference-enforcement [https://perma.cc/B2TL-5PPM].

47. The FCC's recent Report and Order in the 6 GHz band proceeding dismissed concerns about the potential for aggregate interference interfering with point-to-point microwave links from unlicensed devices. However, we are less than sanguine about aggregate interference than the Commission given the rapidly increasing densification of wireless systems. *See* Report and Order and Further Notice of Proposed Rulemaking, In the Matter of Unlicensed Use of the 6 GHz Band, FCC 20-51, 28. https://docs.fcc.gov/public/attachments/FCC-20-51A1.pdf [https://perma.cc/2BNV-FF7E].

48. Bruce Schneier, *Internet Hacking Is About to Get Much Worse*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/opinion/internet-hacking-cybersecurity-iot.html [https://perma.cc/2GJN-8KVW].

promote a better economic use of spectrum. While this would be a somewhat novel approach to wireless policy, other agencies have used similar incentives before.

As part of a dual effort to stimulate the economy and reduce carbon emissions, the Obama Administration promulgated the Car Allowance Rebate System, commonly known as the "Cash for Clunkers" program.[49] Under this program, consumers who turned in old cars that fell below certain efficiency requirements could receive cash rebates to purchase more environmentally friendly vehicles.[50] The program created tremendous demand while in effect, quickly exhausting the program's funding.[51]

Despite successes in improving the overall efficiency of vehicles on the road and reducing carbon emissions, the Cash for Clunkers program was not continued beyond the first year.[52] Some critics pointed out that despite beneficial environmental impacts, the program's costs exceeded its economic benefits.[53] One study suggested that most of the participants would have purchased a new vehicle even without the rebate and another highlighted that the increase in sales spurred by the program was followed by a sharp decline in sales following the end of the program.[54]

The National Telecommunications and Information Administration (NTIA) ran a similar program to facilitate the transition to digital TV. The "TV Converter Box Coupon" program offered consumers coupons to incentivize purchasing equipment that was used to facilitate the transition to digital

49. Consumer Assistance to Recycle and Save Act of 2009 (CARS), Pub. L. No. 111-32, 123 Stat. 1859, 1909–15; *see also* Jennifer Liberto, *Cash for Clunkers Extension Signed into Law*, CNN (Aug. 7, 2009), https://money.cnn.com/2009/08/07/autos/clunkers_continues/ [https://perma.cc/7MCB-P95P].

50. Liberto, *supra* note 49.

51. Bunkley, *supra* note 35.

52. *Id.*

53. *Id.*

54. Ted Gayer & Emily Parker, *Cash for Clunkers: An Evaluation of the Car Allowance Rebate System*, BROOKINGS 7 (Oct. 13, 2013), https://www.brookings.edu/wp-content/uploads/2016/06/cash_for_clunkers_evaluation_paper_gayer.pdf [https://perma.cc/KEM8-5NVK] (finding that the program did not spur new sales); Mian & Sufi, *supra* note 4, at 1107.

broadcasting.[55] Similar incentives could be offered to achieve a number of other goals in spectrum management.

For example, a device-collection fund might be established to mitigate interference issues under new spectrum modalities like CBRS. In CBRS, incumbent and priority license holders share spectrum with generally authorized—essentially unlicensed—users.[56] Such regimes are built on technologies like automated-frequency coordination (AFC) that facilitate greater spectrum sharing. While AFC technology allows for more efficient use of spectrum, it also presents new risks that buyback programs could help solve. For example, AFC devices might malfunction in ways that could cause interference with licensed users. Especially where these devices are widely deployed among the general public, it could become necessary to facilitate the collection of a large number of devices to protect priority licensed users. An effective way of doing so would be to provide a financial incentive to consumers to return these devices.

Another potential use of device collection programs could be an auction designed to facilitate the transition of spectrum currently occupied by unlicensed users—or any band with a large number of consumer devices. Because of the large number of consumer-owned devices, it is currently impractical to transition spectrum away from an unlicensed allocation. Under this hypothetical auction, a device collection fund could be used to incentivize consumers or bounty hunters to find and return specified devices. Clearing devices from a band could prevent the potential for interference or accelerate the adoption of new technologies. Use rights to a particular band or type of use would be sold in a forward auction, and then those funds would be used to fund the collection of devices. In essence, this system would be similar to payments given to users who surrender their spectrum rights under an auction to fund the conversion or purchase of new equipment.

This style of auction would be best suited to clearing bands occupied by outdated or economically inefficient allocations. For example, Wi-Fi and Bluetooth are both versatile platforms that could accommodate a number of existing technologies that

55. *See* NTIA Digital-to-Analog Converter Box Coupon Program, 47 C.F.R. § 301 (2005).

56. *3.5 GHz Band Overview*, *supra* note 5.

currently use their own unique radio channels.[57] Consolidating technologies into a single platform like this might not be prudent today but could become necessary to prevent future interference with valuable services, such as GPS. Facilitating this kind of bargaining might become necessary to properly manage new modalities like CBRS that blur the line between licensed and unlicensed use.

It is worth noting that this approach does assume that some unlicensed users—or coalitions thereof—would be willing to participate in such an auction. Given that unlicensed device manufacturers are not accustomed to paying for spectrum, these companies are likely to be unwilling at first. However, as spectrum becomes increasingly scarce and crowded, unlicensed device manufacturers might decide that pooling resources to expand unlicensed spectrum is within their collective self-interest. For example, the Wi-Fi Alliance has repeatedly asked the Commission to allocate more spectrum for unlicensed use.[58] As the industry group for wireless internet device manufacturers, the Wi-Fi Alliance could pool funds from member companies to bid on a chunk of spectrum to expand the available spectrum for wireless internet.

Relatedly, one proposal to solve collective action problems and promote effective bargaining between spectrum neighbors is for the Commission to facilitate the establishment of "band agents."[59] These agents would hold rights to negotiate the contours of spectrum rights but would not hold any property rights in the spectrum itself.[60] An additional responsibility for agents could be to facilitate device collection programs that facilitate bargaining either within or between "agencies" for different classes of users. These band agents could also help

57. For example, some automobile manufacturers have begun offering options that allow for consumers to use their phone, instead of a traditional wireless fob, to access and control their vehicle. *See Use your iPhone or Apple Watch as a car key*, APPLE (Mar. 16, 2021), https://support.apple.com/en-us/HT211234 [https://perma.cc/3NYW-PB82].

58. *See generally* Alex Roytblat, Comments of Wi-Fi Alliance, *Unlicensed Use of the 6 GHz Band*, GN Docket No. 17-183 (filed July 29, 2020), https://ecfsapi.fcc.gov/file/106291505618623/6%20GHz%20FNPRM%20Comments.pdf [https://perma.cc/QCX5-NDBJ].

59. J. PIERRE DE VRIES & PHILIP J. WEISER, UNLOCKING SPECTRUM VALUE THROUGH IMPROVED ALLOCATION, ASSIGNMENT, AND ADJUDICATION OF SPECTRUM RIGHTS, HAMILTON PROJECT & BROOKINGS, 2, 6, 15 (2014).

60. *Id.* at 17.

facilitate buyback programs to remove devices that are causing interference with users in a particular band.

Advances in wireless technology offer tremendous potential but also create new risks that must be managed. The promise of new technologies—like autonomous vehicles—may transform our cities, but the introduction of these technologies increases the risks of harmful interference. In a crowded spectrum ecosystem, it could become necessary to develop methods of identifying and removing devices likely to cause interference, especially where interference threatens public safety. Buyback programs—whether run by device manufacturers, band agents, or the Commission itself—could be an effective tool for helping manage these risks.

III. COULD BUG BOUNTIES BE ADAPTED TO AID IN THE IDENTIFICATION AND RESOLUTION OF WIRELESS VULNERABILITIES?

Software bug bounties programs have recently gained popularity as a way of offering researchers the chance to receive a reward for identifying security flaws in a Web application or software platform.[61] These programs have become an essential part of security strategies for both public and private organizations.[62] Bug bounties are usually aimed at identifying vulnerabilities that are unknown to developers, which can pose a great threat to security.[63] As such, bug bounties offer substantial rewards as an incentive to conduct research and help address vulnerabilities. Beyond the financial incentive, some

61. *See generally* Fryer & Simperl, *supra* note 3.

62. *See* Marino, *supra* note 6; *see also* Joseph Marks, *The Cybersecurity 202: DARPA wants hackers to try to crack its new generation of super-secure hardware*, WASH. POST (June 8, 2020), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/06/08/the-cybersecurity-202-darpa-wants-hackers-to-try-to-crack-its-new-generation-of-super-secure-hardware/5edd383d88e0fa32f82346f1/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202 [https://perma.cc/R3UT-DKZC].

63. SERGE EGELMAN ET. AL, *MARKETS FOR ZERO-DAY EXPLOITS: ETHICS AND IMPLICATIONS*, *IN PROCEEDINGS OF THE 2013 NEW SECURITY PARADIGMS WORKSHOP* 4–6 (2013), https://www.guanotronic.com/~serge/papers/nspw13.pdf [https://perma.cc/H4RX-8GKZ] (discussing ethical issues and implications related to markets for zero-day exploits).

bug hunters participate in these programs for the professional notoriety.[64]

Despite being widely used in the world of software, bug bounties have yet to be used to address vulnerabilities in wireless systems such as jamming, spoofing, or sniffing.[65] These vulnerabilities might include:

(a) using a combination of jamming and spoofing to interfere with devices like autonomous vehicles and UAVs through sensor inputs[66];

(b) spoofing messages from public safety systems like the Wireless Emergency Alert system to infiltrate Presidential alerts[67];

(c) or using devices to sniff data on a wireless network and to further manipulate it.[68]

Similar to existing bounty programs, security researchers are incentivized to identify these vulnerabilities in private or public systems by the potential of a financial reward. Another key factor in the success of a bug bounty program is clear rules and guidelines for researchers to follow to obey the law. Existing bug bounty programs already face issues from laws such as the Computer Fraud and Abuse Act (CFAA), but a wireless bug bounty program will also need to carefully define how to handle

64. *See* Marino, *supra* note 6.

65. Hui Hu & Na Wei, *A study of GPS jamming and anti-jamming*, *in* 2ND INT'L CONF. ON POWER ELECS. & INTELLIGENT TRANSP. SYS. 388–91 (Dec. 19–20, 2009), https://ieeexplore.ieee.org/document/5406988 [https://perma.cc/BH7D-RVXP] (describing jamming attacks); Ying Ying Chen et. al, *Detecting and Localizing Wireless Spoofing Attacks*, *in* 4TH ANNUAL IEEE COMMUNICATIONS SOCIETY CONFERENCE ON SENSOR, MESH & AD HOC COMMUNICATIONS & NETWORKS 193–202 (June 18, 2007), https://ieeexplore.ieee.org/document/4292831 [https://perma.cc/D6JC-JPVB] (describing spoofing attacks); Hal Berghel, *Wireless Infidelity I: War Driving*, 47 COMMC'NS ACM 21–26 (2004), https://dl.acm.org/doi/pdf/10.1145/1015864.1015879 [https://perma.cc/T6MY-D6DB] (describing sniffing attacks).

66. *See* DREW DAVIDSON ET AL., CONTROLLING UAVS WITH SENSOR INPUT SPOOFING ATTACKS (Aug. 2017), https://www.usenix.org/system/files/conference/woot16/woot16-paper-davidson.pdf [https://perma.cc/MNA6-U634].

67. *See* GYUHONG LEE ET AL., *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks*, *in* MOBISYS '19: PROCEEDINGS OF THE 17TH ANNUAL INTERNATIONAL CONFERENCE ON MOBILE SYSTEMS, APPLICATIONS, AND SERVICES (Association for Computing Machinery 2019), https://dl.acm.org/doi/pdf/10.1145/3307334.3326082.

68. *See* Berghel, *supra* note 65.

liability for violating various FCC regulations. The clearer the rules for security researchers, the better.

In the 1990s', Netscape tested a bug bounty program by offering rewards for researchers who identified flaws in the Navigator browser.[69] Bug bounty programs have seen a resurgence in recent years as major platforms like Google and Mozilla have integrated these programs into their security strategy.[70] Apple recently announced, in an effort to make it easier to find and report bugs, it will offer specialized phones for verified security researchers[71]

Following the success of these programs in the private sector, government entities have started issuing bounties for bugs in critical public safety systems. The Department of Defense and the Department of Homeland Security both offer bounties for vulnerabilities in national security software platforms.[72] The Defense Advanced Research Projects Agency (DARPA) recently offered a bounty for vulnerabilities in new hardware designed for critical systems, like medical databases and voting machines.[73] The State Department has also offered a $10,000,000 reward for any researchers who provide information on "illegal cyber activities" aimed at interfering with US elections.[74]

The potential risks from wireless vulnerabilities could easily justify similar kinds of bounty programs. As already discussed, vulnerabilities in public safety systems would certainly justify the issuance of bug bounties, either by the government or private firms that manufacture the underlying technology. For example, a commercial survey drone recently

69. Fryer & Simperl, *supra* note 3, at 273.

70. *Id.*

71. Haslam, *supra* note 8.

72. *See DoD Vulnerability Disclosure Policy*, HACKERON (Nov. 2016), https://hackerone.com/deptofdefense?type=team [https://perma.cc/5ATY-SUUB]; Maggie Hassan & Rob Portman, *Why We're Encouraging Ethical Hackers to Try and Hack the Department of Homeland Security*, TIME (June 30, 2017, 10:31 AM), https://time.com/4837557/hackers-homeland-security-cyber-attacks/ [https://perma.cc/N9LB-EEUM].

73. Marks, *supra* note 62.

74. Catalin Cimppanu, *US offers $10 million reward for hackers meddling in US elections*, ZDNET (Aug. 5, 2020), https://www.zdnet.com/article/us-offers-10-million-reward-for-hackers-meddling-in-us-elections/ [https://perma.cc/NS9Z-MFN2].

crashed in the United Kingdom due to GPS interference.[75] While nobody was injured in the crash, the report indicated that this type of interference could have potentially lethal consequences.[76] To prevent this kind of harmful interference, manufacturers could offer bug bounties for finding flaws in their own technology, or the government might offer bounties for helping find flaws in GPS to help protect their own use of the technology.

Another frightening possibility for wireless interference could include attacks on autonomous vehicles that use wireless sensors.[77] Through a combination of jamming and spoofing, it could be possible to trick autonomous vehicles into crashing. In 2015, a pair of security researchers identified a critical wireless vulnerability in the OnStar system in Jeep vehicles that allowed for full wireless control of the vehicle, overriding the driver's controls at the wheel.[78] As wireless technology is integrated into more vehicles on the road, the dangers of this type of hacking will only increase.

While bug bounties could have tremendous potential for promoting wireless security, the Commission and other regulators will need to clarify the scope of legal liability when conducting research. Under existing programs, researchers often violate federal laws like the CFAA that prohibit accessing systems without authorization or exceeding authorized access.[79] Companies that offer bug bounties often negotiate agreements

75. Dana A. Goward, *GPS interference crashed a survey drone in the UK. Will the debate resonate in the US?*, RESILIENT NAVIGATION AND TIMING FOUND. (Jul. 20, 2020), https://rntfnd.org/2020/07/20/gps-interference-crashed-a-survey-drone-in-the-uk-will-the-debate-resonate-in-the-us-c4isrnet-ligado/ [https://perma.cc/DNV4-XAMP].

76. *Id.*

77. These kinds of wireless attacks have already been proven possible for UAVs. *See* DAVIDSON, *supra* note 66.

78. *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It,* WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/L7VP-BQGX].

79. *See* 18 U.S.C § 1030; *see also* Naomi Gilens & Jamie Williams, *Federal Judge Rules It Is Not a Crime to Violate a Website's Terms of Service*, ELEC. FRONTIER FOUND. (Apr. 6, 2020), https://www.eff.org/deeplinks/2020/04/federal-judge-rules-it-not-crime-violate-websites-terms-service [https://perma.cc/NAE4-Y8DT].

with researchers to forego prosecution of claims under the CFAA– in addition to providing a reward for their efforts.[80]

Wireless bug hunters might also violate FCC regulations, such as those against creating harmful interference with licensed services.[81] When defining the scope of liability, the Commission should strive to give the broadest possible definition of "good-faith" to ensure no chilling impact on valuable research.

As regulators grapple with how to best approach security research, one good example of how *not* to proceed is the current process for obtaining authorization for research under the Digital Millennium Copyright Act.[82] Occasionally, security research necessitates circumventing "technological protection measures" (TPM) designed to control access to copyrighted material.[83] When researchers wish to conduct research that requires circumvention of the TPM, they must first apply for specific authorization from the Copyright Office.[84] The Ninth Circuit recently allowed a First Amendment challenge to this process.[85] Rather than requiring researches to acquire authorization to conduct specific types of security research, the Commission should create a broad definition of "good-faith" that allows for more valuable research.

One agency that has been relatively supportive of—rather than outright hostile towards—security research is the Department of Justice (DOJ). The DOJ has published guidelines that gives some context for how the agency approaches enforcement of the CFAA to give some guidance to researchers

80. *DANIEL ETCOVITCH & THYLA VAN DER MERWE, COMING IN FROM THE COLD A SAFE HARBOR FROM THE CFAA AND THE DMCA § 1201 FOR SECURITY RESEARCHERS*, (2018), https://dash.harvard.edu/bitstream/handle/1/37135306/ComingOutoftheCold_FINAL.pdf?sequence=1&isAllowed=y [https://perma.cc/S24P-D2FA].

81. 47 C.F.R. § 27.64 (2013).

82. *See generally* U.S. COPYRIGHT OFF., RULEMAKING PROCEEDINGS UNDER SECTION 1201 OF TITLE 17, https://www.copyright.gov/1201/ [https://perma.cc/P6G6-AYK5].

83. *See* Ed Felten & J. Alex Halderman, Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201, 1, 6–9 (Dec. 12, 2017), https://cdn.loc.gov/copyright/1201/2018/comments-121817/class10/class-10-initialcomments-felten-halderman.pdf [https://perma.cc/PL7B-PB76].

84. *Id.*

85. Green v. U.S. Dept. of Justice, 392 F. Supp. 3d 68, 76 (D.D.C. 2019).

on how best to steer clear of liability.[86] While the DOJ's guidelines could certainly be clearer, the Department does not place any *ex ante* restrictions on security research.[87] In fact, the DOJ has filed comments with the Copyright Office supporting efforts to expand the security research exception to the DMCA.[88] The DOJ noted that the kind of security research sought by the expansion was "an effective component of efforts to improve the security of devices and technology."[89]

Even where a security researcher does not face the possibility of criminal prosecution under the CFAA, they might still risk the possibility of civil actions from the very companies they are trying to assist.[90] This is because some companies are far less accepting of researchers' attempts to breach their system than others. These concerned companies are potentially weary of the fact that unveiling troublesome vulnerabilities in a particular technology or platform might negatively impact the market or cause financial losses before companies can adequately resolve the problem.

In one recent example, a pair of security researchers who identified vulnerabilities in drones manufactured by DJI were forced to walk away from a bounty after the company threatened litigation.[91] According to the researchers, DJI asked them to sign an allegedly unfair non-disclosure agreement, and when they resisted, DJI threatened them with an action under the CFAA.[92] Companies also routinely use the DMCA as a method

86. *See* U.S. DEP'T JUST. CYBERSECURITY UNIT, LEGAL CONSIDERATIONS WHEN GATHERING ONLINE CYBER THREAT INTELLIGENCE AND PURCHASING DATA FROM ILLICIT SOURCES (2020), https://www.justice.gov/criminal-ccips/page/file/1252341/download [https://perma.cc/7CGJ-7MCM].

87. *Id.*

88. Letter from John T. Lynch Jr., Section Chief, U.S. Dep't of Just., to Regan Smith, Gen. Couns. and Assoc. Reg. of Copyrights, U.S. Copyright Off. (June 28, 2018), https://www.copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf [https://perma.cc/WC2X-8Y97].

89. *Id.* at 6.

90. *See* Jack Cable et al., *Response to Voatz's Supreme Court Amicus Brief*, DISCLOSE.IO (Sept. 14, 2020), https://disclose.io/voatz-response-letter/ [https://perma.cc/3P2Z-T2VA].

91. Amit Elazari, *Hacking the Law: Are Bug Bounties a True Safe Harbor?*, USENIX (Jan. 18, 2018) https://www.usenix.org/conference/enigma2018/presentation/elazari [https://perma.cc/SP9J-3UX3].

92. *Id.*

of preventing or deterring research that could expose critical vulnerabilities in their software that they would rather ignore.[93]

To encourage more valuable security research—especially into wireless vulnerabilities—the Commission should take an approach closer to the DOJ and publish clear guidelines that outline the limits of acceptable research. Critically, the Commission should also avoid placing any *ex ante* restrictions on security research, despite the potential for additional interference. Perhaps one reason why wireless bug bounties have not seen much use—while software bug bounties have become increasingly popular—is the lack of clarity from the Commission with regard to the contours of acceptable research. Researchers might simply steer clear of any project that might require causing harmful wireless interference, out of concern that they will be subject to prosecution despite their good intentions.

If the Commission takes steps to clarify the scope of liability, bug bounties could be instrumental in guaranteeing the safety and security of wireless systems. For private systems like autonomous vehicles, the financial incentives are certainly sufficient to motivate manufacturers to post bounties for any vulnerabilities that could be exploited with potentially tragic results. Tesla notably already has a bug bounty program, but has yet to issue any rewards for wireless vulnerabilities.[94] The government might also post bug bounties for wireless vulnerabilities in critical public safety systems like GPS. The Department of Defense has already issued similar bounties for software systems, so they already have the infrastructure in place to manage such a program.[95]

CONCLUSIONS & RECOMMENDATIONS

Spectrum regulators and telecommunications policymakers tend to prefer creating market solutions to issues before relying on command-and-control style regulations. Supporters of this kind of approach argue that market solutions can effectively manage negative externalities while also leaving sufficient

93. *See generally* Felten & Halderman, *supra* note 83.

94. *See Tesla*, BUGCROWD, https://bugcrowd.com/tesla [https://perma.cc/XWR7-6L9Y] (last visited Sept. 13, 2021).

95. *DoD Vulnerability Disclosure Policy*, *supra* note 72.

breathing room for companies to innovate.[96] In this sense, bounties may have a promising future in telecommunications policy. We have outlined a number of ways in which bounties *might* be used in spectrum regulation, but further study is necessary to evaluate whether these solutions *should* be used. Whistleblower bounties might be an effective tool for aiding in the criminal enforcement of the Telecommunications Act, but 'the success of these kinds of programs depends heavily on the economic incentives. Further studies could be conducted to better understand how to balance economic incentives to create an efficient and effective whistleblower program at the FCC. These studies could also evaluate whether increasing fines for interference or other violations of Commission regulations would actually have the desired deterrent effect.

Buyback programs might be used in a number of ways to address interference issues or to promote the reallocation of spectrum to a more economically beneficial use, but in some sense these programs might be a solution in search of a problem. However, if interference issues become more complicated and common as wireless networks become increasingly crowded, these programs could become instrumental in spectrum regulation. Future studies could attempt to better quantify the potential risks of aggregate interference or other issues like failures in technologies like AFC.

Bug bounties for wireless vulnerabilities could also be used to promote spectrum security, but these programs likely won't see wide use until the Commission clarifies how they will approach enforcement against security researchers. Future studies might evaluate how the Commission should define "good-faith" and what—if any—additional conditions should be placed on security research.

96. *See* Nathan Alexander Sales, *Privatizing Cybersecurity*, 65 UCLA L. REV. 620, 647 (2018).