U.S. Copyright Office

DMCA 1201 Proceeding (2018) Comment and Evidence Submission

Re: Docket no. 2017-10

March 14, 2018

Comment of the "Security Researchers" - Prof. Steven Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science/Law, Columbia University; Prof. Matt Blaze, Associate Professor of Computer and Information Science University of Pennsylvania; Prof. Nadia Heninger, Assistant Professor of Computer and Information Science University of Pennsylvania,

represented by Prof. Andrea M. Matwyshyn, Professor of Law/ Professor of Computer Science (by courtesy) Northeastern University/ Affiliate Scholar, Center for Internet and Society Stanford Law School

--

The Security Researchers take no position on whether the Copyright Office and the Librarian of Congress should grant the request of the proponents of Class 10.

This comment seeks to refute material misstatements and misrepresentations about the 2015 Section 1201 exemption process and voting system security made by opponents to Class 10, Dominion Voting Systems Corporation, a privately-held company headquartered in Toronto, Ontario,[1] Election Systems & Software, LLC, a privately-held company headquartered in Omaha, Nebraska,[2] and Hart InterCivic, LLC, headquartered in Austin, Texas[3] (the "Vendors").

--

1. **The Vendors misrepresent the exemption granted during the 2015 exemption process and the record established in 2015.**

Without any citations to procedural irregularity, the Vendors question the legitimacy of the 2015 exemption process and the appropriateness of the Copyright Office and Librarian of

[1] https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=46054856

[2] https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=96810

[3] https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=430322

Congress in granting the 2015 security research exemption.[4] The Security Researchers strongly object to this unfounded allegation and note that the Vendors had ample opportunity but chose not to participate in the 2015 process.

The Vendors seek to debate the linguistic minutiae of the meaning of the term "consumer"[5] as used in the language of the 2015 exemption.[6] However, the Vendors' definitional argument is entirely inapposite - the granted exemption's express language specifically states that voting systems, in the broadest sense of the term, are included within the exemption's scope. Voting systems were referenced in the record supporting the exemption, both by the Security Researchers[7] themselves based on first-party knowledge from their own research and again by third-party supporters of the exemption.[8] The record is robust. The Copyright Office also

[4] "System Providers question whether the 2015 record, which was largely directed toward typical consumer products, adequately supported creating an exemption for circumvention of voting machine software" Comment of Vendors, 4

[5] "Voting machines are "use[d] by individual consumers" only in the sense that some consumers vote. Voting machines are procured and owned by state and local governments... Voting machines are not consumer products under any typical conception of that term." Comment of Vendors, 3

[6] The Vendors do not offer a citation or a definition for their novel use of the term "consumer good." Their idiosyncratic use is inconsistent with the generally-accepted legal definition for the term as provided in the Uniform Commercial Code. Uniform Commercial Code Section defines "Consumer goods" to mean "goods that are used or bought for use primarily for personal, family, or household purposes." When researchers lawfully purchase or otherwise gain lawful access to voting systems, they are engaging with and have acquired a good for the personal purposes of conducting security research. Further, the Vendors are subject to state consumer protection statutes in the performance of their services. http://www.michigan.gov/documents/buymichiganfirst/6200250_257330_7.pdf Ergo, their customers believe them to be providing goods and services to consumers, and at least one of the Vendors appears to have contractually stipulated that their products and services fall within this characterization.

[7] The Security Researchers have themselves engaged in directly impacted research. https://www.copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_SecurityResearchers_Class25.pdf, 2; 10.

[8] https://www.copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Verified_Voting25.pdf

signaled its unambiguous intention to include voting systems within the exemption with its creation of unique timing for the start of exemption for voting system research, in particular.[9]

2. The Vendors misrepresent the history of inadequate voting system security in the U.S. and the inadequacy of existing testing and safeguards.

As the 2015 record amply demonstrated, vulnerability history affirms that voting system vendors have not successfully identified and corrected all flaws in their products prior to shipping. One vulnerability database currently hold records on over 275 known voting system vulnerabilities in shipped voting systems.[10] The security practices and representations of voting vendors to state officials about security also warrant close third-party technical scrutiny: a whistleblower who is a former Vendor employee has apparently alleged that one of the Vendors has lied to state officials about the security of their voting systems.[11] One of the Vendors also purchased the assets of a now-defunct voting system company,[12] a portion of whose legacy systems[13] had been decertified by the State of California for security reasons.[14] Not all states require rigorous testing of the security of voting systems,[15] and to the extent that security standards exist, they do not always reflect current security practices considered reasonable by security experts and international standards bodies.[16]

3. The Vendors misrepresent the DEFCON Voting Machine Village and the technical reality of voting systems security.

---

[9] Because of the strength of the record, the Copyright Office and the Librarian of Congress identified voting systems research for immediate protection under the exemption. By contrast, the exemption created a one-year lag in commencement for all other security research protected under the exemption.

[10] Interview of Brian Martin, VP of Vulnerability Intelligence, RBS Security.

[11] https://www.wired.com/2008/03/whistleblower-v/

[12] The company in question was implicated in an indictment by Ohio prosecutors for a "worldwide pattern of criminal conduct." https://columbusfreepress.com/article/diebold-indicted-its-spectre-still-haunts-ohio-elections ; http://www.cleveland.com/metro/index.ssf/2013/10/diebold_charged_with_bribing_o.html

[13] https://www.wired.com/2009/03/diebold-admits/

[14] http://www.nytimes.com/2004/05/01/us/high-tech-voting-system-is-banned-in-california.html

[15] https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/

[16] See, e.g., ISO 29147 https://www.iso.org/standard/45170.html and ISO 30111 https://www.iso.org/standard/53231.html

Without citation, the Vendors assert that the DEFCON Voting Machine Village (the "Village") involved "only obsolete machines."[17] This assertion is inaccurate. To our knowledge, at least three of the machine types tested as part of the Village are still in use. Indeed, quite troublingly, Village organizers discovered that one of the purchased machines tested even still contained a memory card of 650,000 actual voters' names and identifying information.[18]

The Vendors further assert that the Village "proved little more than that old voting machines used old technology."[19] This assertion is false. The architectures of the Village machines are still in use in machines currently used for voting; machines in use have the same attack surfaces as the machines made available in the Village.[20] In particular, the issues of foreign-made components in the Village machines and risks of remote compromise continue to impact every voting system with foreign-made components in use today.[21]

Without citation, the Vendors assert incorrectly that voting systems never connect to the internet.[22] Yet, the architecture[23] of one of the machines tested as part of the DEFCON voting village had internal components reflecting internet connection capabilities.[24] Additionally, as a technical matter, some backend voting systems as used and implemented by county officials are attached to the internet. Indeed, as the intelligence community noted, some components of backend systems were impacted remotely through the internet by attackers during the 2016 election.[25]

Without reference to explicit security audit processes, such as, for example, the existence of bug bounty programs or formal third-party bug reporting channels, the Vendors assert that independent technical verification of their systems' security practices is not necessary because

---

[17] Comment of Vendors, 9

[18] https://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462

[19] Comment of Vendors, 9

[20] http://www.crypto.com/papers/blaze-govtreform-20171129.pdf

[21] https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

[22] "Voting machines and election management systems are never connected to the Internet, which prevents any attack from a remote location." Comments of Vendors, 6

[23] https://www.wired.com/story/voting-machine-hacks-defcon/ ("The DefCon Voting Village offered a number of voting models, including a notorious decommissioned WINVote machine from Fairfax, Virginia—a model known for having blatant security flaws such as exposed Wi-Fi vote tallying")

[24] https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

[25] https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html

of legal checks in some state law.[26] Legal compliance checks will never compensate for technical security inadequacy in the system itself, particularly when vendors rely on foreign-made, potentially vulnerable components in their voting systems.[27] For this reason, various state and federal officials attended and participated in the Village.[28] Whether some state laws create particular compliance requirements is irrelevant to whether the Vendors' systems as constructed reflect the technical security properties of confidentiality, integrity, and availability. State laws vary dramatically[29] on compliance requirements,[30] as does the technical capability of state officials to meaningfully verify system security and the accuracy of sales pitches by vendors. But, more directly, if Vendors believe their security processes are adequate, they should welcome third party independent validation as a way to buttress legislators' and the public's trust in their products.[31]

Without citation, the Vendors belittle the Village and DEFCON as a convention for "entertaining the public." [32] Thus, it appears that the Vendors are unfamiliar with both the event and its important role within the security and legal community. Members of Congress,[33]

---

[26] "State and local officials across some 10,000 U.S. jurisdictions implement comprehensive safeguards to protect their election systems, and those measures reinforce those built into election hardware and software." Comment of Vendors, 6

[27] https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf ("Moreover, a closer physical examination of the machines found, as expected, multiple cases of foreign-manufactured internal parts (including hardware developed in China), highlighting the serious possibility of supply chain vulnerabilities.")

[28] For example, U.S. Representative Will Hurd, Congressional Cyber Caucus (R-TX), U.S. Representative Jim Langevin, Congressional Cyber Caucus (D-CT) attended the Village, as well as representatives of the Election Assistance Commission (EAC), Multi-State Information Sharing & Analysis Center (MS-ISAC), National Institute for Standards & Technology (NIST), National Governors Association (NGA), US-Computer Emergency Readiness Team (US-CERT), U.S. Department of Homeland Security (DHS), and U.S. Senate Homeland Security & Governmental Affairs Committee. https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

[29] For example, while some state law requires that machines use paper trails, some state law does not. Recounts are functionally impossible on machines without paper trails.

[30] As the Vendors explained, only "33 states have statutes that prohibit tampering with voting systems." Comment of Vendors, 6

[31] https://www.politico.com/story/2018/02/24/elections-vendors-russia-423435

[32] Comment of Vendors, 12

[33] https://hurd.house.gov/media-center/in-the-news/congressmen-defcon-please-help-us-hackers

representatives of the FTC,[34] DOJ,[35] FDA,[36] intelligence agencies,[37] and other government officials[38] attend DEFCON regularly, give presentations, and participate in panels.[39] The conference operates in a manner parallel to an academic conference with a program committee and formal presentations of research that include demonstrations and slides.[40] One of us – an academic – co-organized the Village. Another of us – also an academic – sits on the program committee of DEFCON as a legal subject matter expert.

The experience of participants in the Village amounted to an experiential learning class in assessing voting systems' security, and it will assist them in working with their local election officials to help them select more secure voting systems in the future. The Village has already inspired participants to generate numerous new creative works, such as articles and blog posts about their experiences in the Village.[41] The Vendors' dismissiveness toward this conference of security experts raises questions about the Vendors' baselines of security knowledge and their receptiveness in general to external reports of security vulnerabilities from security researchers, government officials, and the public.

4. The Vendors misrepresent the dynamics of academic security research into voting systems and incorrectly assess the level of interest among academics in generating creative works about voting systems security.

The Vendors allege that more security research into their products' security and the 2015 exemption are not necessary because "[a]cademic and independent researchers have also conducted research into election systems prior to the 2015 exemption for security research." Indeed, some voting security research did occur prior to 2015 – the Security Researchers are some of the academics who conducted it. It was precisely because of the troubling and restricted nature of these pre-2015 voting security research experiences and the severity of the security vulnerabilities unearthed during even such limited pre-2015 research that motived the

---

[34] https://www.ftc.gov/news-events/events-calendar/2017/07/cmr-mcsweeny-panel-meet-feds-defcon

[35] https://www.defcon.org/html/defcon-25/dc-25-speakers.html#Feds

[36] https://www.defcon.org/html/defcon-25/dc-25-speakers.html#Feds

[37] https://www.cnet.com/news/nsa-director-finally-greets-defcon-hackers/

[38] https://gcn.com/articles/2016/08/12/defcon-meet-feds.aspx

[39] https://www.youtube.com/watch?v=nQCqQ8etoDE

[40] https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/

[41] See, e.g., https://www.alienvault.com/blogs/security-essentials/how-the-vote-hacking-was-done-at-defcon-25 ; http://securityaffairs.co/wordpress/61507/hacking/def-con-us-voting-machines.html ; https://www.thesecurityblogger.com/defcon-hackers-find-its-very-easy-to-break-voting-machines/ ;

Security Researchers to request the 2015 security research exemption. The more we researched, the more the severity of the security inadequacy of many voting systems became apparent.

The Vendors also allege, again without citation, that "[w]aning academic interest in hacking old voting machines raises a substantial question about what noninfringing research purpose is being affected by Section 1201." Allow us, as academics who research voting systems security and as the proponents of the 2015 security research exemption to assure the Vendors that the interest of academics in voting system security is definitely not waning. In particular, interest in voting security is on the rise, not only among computer scientists but also among law professors, who now collaborate with computer scientists on auditing and improving the (currently inadequate) security of the electoral process as a whole. These collaborations have already resulted in new creative works as a result of the existence of the 2015 security research exemption.