October 10, 2018

Office of the Attorney General
Consumer Protection Division
PO Box 12548
Austin, TX 78711-2548

Re: Epson Pushing Firmware Upgrades That Disable Third-Party Ink Usage

To whom it may concern,

I am a Senior Staff Attorney at the Electronic Frontier Foundation, a nonprofit public interest organization that defends the rights of technology users. It has come to our attention that Epson (a company best known for its printers and accompanying inks) may be engaging in misleading, deceptive, or anticompetitive behavior, to the detriment of Texas consumers. In particular, EFF has received reports—from, among others, a resident of Texas—that Epson has issued firmware updates to prevent owners of Epson printers from using third-party ink supplies.

While printer manufacturers often sell ink cartridges for use in their printers, it is generally possible to use third-party substitutes for these cartridges. In addition to buying standard ink cartridges from a third party, a customer may also prefer to refill an empty cartridge from the printer company, or use third-party refillable cartridges, or switch from cartridges to a continuous ink supply system.[1] Each of these options can offer consumers significant advantages in terms of both price and convenience.

It appears, however, that around late 2016 or early 2017, Epson began issuing firmware updates to some printer models to prevent customers from using third-party ink options. Firmware updates are delivered over the Internet and change the software embedded in the printer, thereby changing the behavior of printers after they have been purchased. While firmware updates can fix bugs, add features, or improve security, they can also restrict a printer's functionality. Essentially, the updates at issue change the way Epson printers read the chips used in refilled cartridges, third-party cartridges, and continuous ink supply systems. After being updated, affected Epson printers will only recognize and accept new Epson-brand ink cartridges.

[1] A continuous ink supply system avoids cartridges altogether by connecting high-capacity ink tanks to the printhead in the printer. This option is especially suited to high-volume users who depend on the convenience of uninterrupted printing.

It is not clear that customers were informed when buying an Epson printer that their ability to use third-party ink options could or would be later disabled. Moreover, it does not appear that Epson informed customers when it sent the firmware update that it would disable third-party alternatives to Epson cartridges. Epson's conduct may therefore be misleading or deceptive within the meaning of the Deceptive Trade Practices-Consumer Protection Act. *See* Tex. Bus. & Com. Code Ann. § 17.46(a) (West 2018). In addition, the later restriction of third-party ink options may fall within the specific examples of prohibited behavior enumerated in section 17.46(b)(13) ("knowingly making false or misleading statements of fact concerning the need for parts, replacement, or repair service") and section 17.46(b)(24) (prohibiting nondisclosure of information intended to induce a purchase).

Disabling third-party ink options has a detrimental impact on both Texas consumers and third-party ink manufacturers. When restricted to Epson's own cartridges, customers must pay Epson's higher prices, while losing the added convenience of third-party alternatives, such as refillable cartridges and continuous ink supply systems. This artificial restriction of third-party ink options also suppresses a competitive ink market and has reportedly caused some manufacturers of refillable cartridges and continuous ink supply systems to exit the market.[2]

Nor are the practical consequences of this conduct limited to its impact on consumers and the market. Rather, using firmware updates to remove functionality that consumers desire threatens harm to the security of the Internet. Printers sometimes have security vulnerabilities, which, when found, can be exploited—for example, to remotely execute computer code.[3] Home devices that have been thus infected can be used to spy on their owners' local networks, or as a launching point for attacks on other computers. For example, home devices infected by the Mirai malware were used to shut down large portions of the Internet's key infrastructure in 2016.[4] Firmware upgrades are a common way for manufacturers to fix these vulnerabilities. But if customers come to believe that firmware updates, without warning, might also disable their ability to use third-party ink options, they might choose to forgo updates altogether. Left unpatched, printer vulnerabilities weaken security across computers and networks connected to affected

---

[2] *See* http://www.printerfillingstation.com/Ink_Refills/Epson/61-E.htm. While the Deceptive Trade Practices-Consumer Protection Act does not specifically reference anticompetitive behavior, section 17.46(c)(1) provides that section 17.46(a) be construed in accordance with interpretations of section 5(a)(1) of the Federal Trade Commission Act (codified at 15 U.S.C. § 45(a)(1)), which in turn prohibits "[u]nfair methods of competition in or affecting commerce." Bus. & Com. § 17.46(c)(1).

[3] *See, e.g.*, Ms. Smith, *Hundreds of HP Inkjet Printer Models Vulnerable to Critical Remote Code Execution Flaws*, CSO Online (Aug. 6, 2018), https://www.csoonline.com/article/3295012/security/hundreds-of-hp-inkjet-printer-models-vulnerable-to-critical-remote-code-execution-flaws.html.

[4] *See* https://en.wikipedia.org/wiki/Mirai_(malware)#Use_in_DDoS_attacks.

printers. Even people who are not themselves Epson customers could be vulnerable to an exploit if they connect to a network that includes an unpatched printer.

As such, Epson's reported practice of using firmware updates to prevent the use of third-party ink options is potentially misleading, anticompetitive, and dangerous. We therefore urge the consumer protection division—pursuant to sections 17.60 and 17.61 of the Deceptive Trade Practices-Consumer Protection Act—to investigate Epson's advertising, firmware updates, and other practices with respect to disabling third-party ink options. And, if warranted by the investigation, we would further encourage the consumer protection division to bring an action under section 17.47, or, at the very least, to seek an assurance of voluntary compliance under section 17.58.

Thank you for your time and consideration in this matter. We hope this information proves helpful in protecting Texas consumers.

Respectfully submitted,

Mitchell L. Stoltz
Senior Staff Attorney
Electronic Frontier Foundation