ITIF
The Information Technology
& Innovation Foundation

Should Government Regulate Illicit Uses of 3D Printing?

BY DANIEL CASTRO | MAY 2013

Most technologies can be used for negative purposes—steel can be used to make knives that can then be used as weapons, but that does not mean the government should take us back to the Stone Age.

Additive manufacturing, or 3D printing, is a process used to create a physical object from a digital model by laying down (i.e. "printing") successive layers of materials. The technology is useful because it allows rapid prototyping, reduces waste in the manufacturing process, and offers design flexibility. While 3D printing technology has been around for a while, prices are dropping to the point that it is feasible for consumers to have it in their homes (you can buy a 3D printer on Amazon for about $1,500).[1] And prices will continue to drop. This means that some kinds of physical objects—even those that may have been difficult or illegal to obtain in the past—can now be produced by anyone with access to a 3D printer and the right information. However, since the technology moves production of certain goods from the hands of a relatively small number of manufacturers to a much larger number of citizens, it will be much more difficult for government to regulate the production of these goods.

Recently, these issues have come to a head. On May 5, Defense Distributed, a nonprofit organization dedicated to producing and distributing the technical blueprints needed to enable 3D printing of firearms, announced that it had released a free computer-aided design (CAD) file for "the Liberator"—the first fully-3D printable gun.[2] Before then, it had already produced and shared files that allow users to print rifle magazines, ammunition, grenades, and silencers.[3] Four days later, Defense Distributed announced that the U.S. Department of State's Directorate of Defense Trade Controls had ordered it to take down these files because distributing them online was a violation of the International Traffic in Arms Regulation (ITAR).[4]

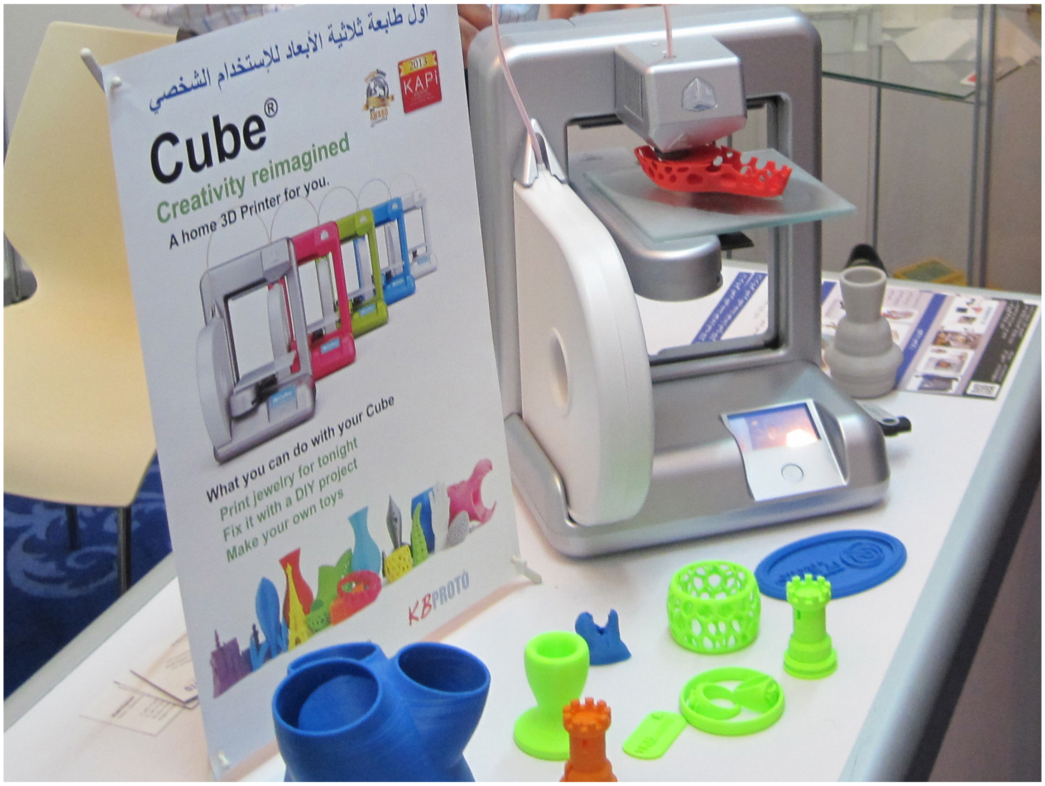
اول طابعة ثلاثية الأبعاد للإستخدام الشخصي
Cube®
Creativity reimagined
A home 3D Printer for you.
2013
KAPI
What you can do with your Cube
Print jewelry for tonight
Fix it with a DIY project
Make your own toys
KBPROTO

Figure 1: The Cube is a low-cost 3D printer available to consumers. (Photo by author.)

For those who remember the "Crypto Wars"—when the government tried to control the use and export of certain types of cryptography—the use of the ITAR to take down gun designs for 3D printers probably seems like an unwelcome blast from the past. During the Crypto Wars, the U.S. government argued that distributing certain cryptographic software was a violation of federal export restrictions on munitions. The creators of these cryptographic tools generally countered that their software was protected speech under the First Amendment (an argument that has generally been supported by the courts).[5] In addition, the government found that its efforts to control the distribution of prohibited cryptographic software were largely ineffective, since it could be so easily copied and shared online. Thus, it is a bit surprising to see the government use the ITAR to request that a website remove designs for 3D printed guns. First, such a prohibition is likely to be ineffective (the blueprints for "the Liberator" are now available on many other websites, including The Pirate Bay). Second, if Defense Distributed applied geo-location restrictions on its content such that only individuals in the United States could download its CAD files, the ITAR restrictions would likely not apply (since it would no longer be "exporting" the files).

Gun control advocates naturally are dismayed at the potential implications of unregulated 3D printing. It's not that individuals cannot already produce weapons without 3D printers—a good machinist with enough time, skills, and resources could probably replicate many weapons (and there are even various websites and books instructing amateurs how to create homemade guns). The difference is that 3D printing drastically reduces the barriers to production. Moreover, if anyone with access to the Internet and a 3D printer can produce working guns and ammunition, many gun control measures, such as licenses and registration, marking requirements (e.g. serial numbers), and detection (e.g. metal detectors and x-ray scanners) could be circumvented on a large scale. In addition, since most gun laws focus on regulating the purchase of weapons or the production of guns by a licensed manufacturer (rather than by individuals), existing laws do little to regulate 3D printing of weapons at home.

While the dominant issue right now is about 3D printing of weapons, similar policy issues will also arise if the government wants to restrict citizens from producing other types of objects with 3D printers, such as items that infringe on the intellectual property rights of others. After all, 3D printing allows individuals to produce high-quality replicas of other items, such as designs for furniture or household goods. For example, the Lego Group may object if some consumers begin to use 3D printers to produce their own counterfeit toys that are exact duplicates of the official Lego products, and LucasFilm may object to consumers producing unlicensed Star Wars merchandise. In addition to using peer-to-peer file sharing services to illegally download music, movies, and software, consumers may also begin to pirate physical goods by downloading CAD files from these services. In this regard, 3D printing likely will reignite many of the debates raised by other copying technologies, such as photocopiers, VCRs, and Napster.

Figure 2: The Pirate Bay might replace Ikea as Sweden's top exporter of modern design. (Photo by Flickr user "Scorpions and Centaurs".)

If governments want to control the use of 3D printing technology, at what points should they enforce control? To answer this question, let's first consider the types of interventions that are possible. Then, we will discuss which interventions make the most sense given what we have learned from past efforts to regulate copying technologies.

POLICY OPTIONS

There are three levels at which government could try to regulate 3D printing: the printed items, the information, and the 3D printers.

First, government can regulate the final 3D-printed products. For example, the government could restrict possession of 3D-printed guns or ammunition. We already have some laws like this in place. The Undetectable Firearms Act, passed in 1988, prohibits gun makers from manufacturing guns that cannot be detected by metal detectors and x-ray machines. This legislation has been extended once, but is set to expire in December 2013.[6] In addition to calling for reauthorization of the ban, lawmakers have proposed legislation to explicitly outlaw the production of such weapons in the home.[7] In January of this year, New York Congressman Steve Israel (D-NY) called for new legislation to prohibit consumers from using 3D printing to make high capacity magazines and guns.[8] This type of approach has precedent as laws already restrict ownership of certain types of goods. As with similar efforts to prohibit individual behavior, such as growing marijuana in small amounts at home, enforcement is difficult. However, such measures can be a deterrent.

Second, government can restrict selling, distributing, accessing, or possessing certain information. When domestic intermediaries provide access to restricted information, regulation can be easy. Getting content removed from a website like DEFCAD is straightforward since it is a non-profit based out of Texas and the individuals operating the website are U.S. citizens. Similarly, the government could coerce compliance with a notice-and-takedown regime for any illicit 3D printing blueprints for websites hosted in the United States or by U.S.-based organizations.

But even if the government restricts domestic organizations from selling 3D printing designs for illicit goods (just as it restricts organizations from hosting other types of illegal digital content), it cannot restrict those operating outside of its jurisdiction. If this information is hosted outside of the United States or distributed enough in nature that there is no clear entity to take enforcement action against (e.g. an anonymous peer-to-peer network), then restricting access to this type of information becomes much more difficult. Certainly, other measures can be used, such as blocking access to the sites hosting this content, but past efforts to implement these types of measures during the SOPA/PIPA debate were politically unpopular.

If the government cannot regulate intermediaries from disseminating the information, it can outlaw possession of the information itself. In this case the government would go after individual users simply for having banned information, such as it does for possession of child pornography. Not surprisingly, attempts by government to control access to information often become contentious because of concerns about censorship and violations of free speech. But again, there is precedent. Governments already make it illegal to possess certain types of weapons-related information. For example, regardless of whether it is in a book or on the Internet, it is illegal to disseminate instructions on how to make certain types of explosives or weapons of mass destruction.[9] Still, because this is such a contentious free speech issue, it is not likely that Congress will pursue this path for 3D technology.

(Already Congressman Israel has made it clear that he does not want penalize individuals for downloading plans for 3D printed guns, only for actually printing them.[10])

Third, government can regulate 3D printers by controlling how they are manufactured, how they are used, or who can buy them. Government could require that the companies that produce 3D printers adhere to certain standards. For example, 3D printers might be required to embed some kind of unique identifier on all objects created by them so they can be traced. In the past, policymakers have proposed various types of mandatory digital rights management (DRM) technology to control the use of copying technologies, such as the Digital Audio Recorder Act of 1987, which mandated DRM for digital audio tapes, and the Perform Act of 2007, which did the same for digital audio transmissions. A similar type of countermeasure has been used to prevent counterfeiting paper banknotes, partially through voluntarily measures by the private sector. To discourage individuals from using high-quality printers to counterfeit money, many printer companies have included steganography technology with their color laser printers that embeds a serial number and time stamp in tiny yellow dots on all printouts.[11] Similarly, software companies such as Adobe include a counterfeit deterrence system in their graphics editing programs to prevent users from illegally copying paper currency.[12] Congressman Israel has said that this type of DRM-like countermeasure is off the table for legislation.[13]

Alternatively, government could require a license, registration, or background check to own a 3D printer. While a policy like this is conceivable—after all, the government requires permits for many other things and the idea of an "Internet driver's license" continues to crop up from time to time—it seems both unlikely and ill-advised because of the intrusiveness and complexity of such a requirement.

POLICY RECOMMENDATIONS

While new technology may introduce new risks, it should not necessarily change the rules. For example, with regards to the gun debate, if professional gun makers are not allowed to make undetectable, unmarked guns, then amateur gun makers at home should not be allowed to make them either. Similarly, if individuals are not allowed to carry a concealed handgun without a permit, it should not matter if it was bought from a dealer or made at home using a 3D printer. Likewise, since it is illegal to create counterfeit goods, this should not change simply because it is easier to do so with 3D printers. Although 3D printing opens up new practical challenges, especially around enforcement, the policy questions for 3D printers are not substantively different than for other technologies. Since we have been down this road before, it is worth remembering the big lessons from the past.

- Do not try to stop innovation
- Encourage voluntary actions by Internet stakeholders
- Regulate intermediaries when necessary
- Remember that a policy can be effective without being perfectly enforceable

Do not try to stop innovation

The most important lesson from past policy debates on copying technologies, whether they are analog or digital, is not to try to block the technology itself. We have likely only begun to touch the potential of 3D printing, and while some current and potential uses are of concern, it has a vast array of legitimate and beneficial uses that should be explored. The United States should strive to be the leader in the use of innovative technologies such as 3D printing and that is possible only if these technologies are widely available and allowed to evolve and improve. Most technologies can be used for negative purposes—steel can be used to make knives that can then be used as weapons, but that does not mean the government should take us back to the Stone Age. Similarly, even though it may have some concerns, government should not impede the development of a general-purpose technology like 3D printing.

Encourage voluntary actions by Internet stakeholders

Sometimes self-regulation is better than government intervention. Rather than create new laws and regulations, the government should encourage voluntary actions by stakeholders. This can be particularly useful when threats change rapidly and private-sector actors are better able to adapt to shifting conditions. For example, MakerBot, a producer of 3D printers, started the website Thingiverse in 2008, giving individuals a platform to share files that allow users to create different objects on 3D printers. However, early on, they decided to limit the types of materials that could be posted. The company's acceptable use policy prohibits many types of illegal or objectionable content.[14]

Relying on the private sector does not mean that government has no role. For example, the Central Bank Counterfeit Deterrence Group, an international group of 32 central banks, provides support for the anti-counterfeiting technology used by hardware and software companies to reduce counterfeit currency. Similarly, the Department of Homeland Security's Office for Bombing Prevention runs the Bomb Making Materials Awareness Program intended to help private-sector employees identify and report suspicious behavior.[15] By acting as a convener and thought leader, the government can help the private sector deal with new challenges.

Regulate intermediaries when necessary

Sometimes government intervention is necessary. For example, while MakerBot has refused to allow users to post weapons on its site, groups like Defense Distributed have raised money to create competing sites like DEFCAD specifically for this purpose. If self-regulation is ineffective, then government enforcement may become necessary. In this case, the government might require websites to adhere to a notice-and-takedown regime for certain CAD files, such as those that pose a threat to public safety or infringe on intellectual property rights. Although some actors may be outside the jurisdiction of the United States, there are typically intermediaries on the Internet such as ad networks, payment processors, Internet service providers (ISPs), and search engines, which can be regulated.

Remember that a policy can be effective without being perfectly enforceable

Threats to public safety and intellectual property rights are global problems, and 3D printing introduces new risks. As noted earlier, because of the distributed nature of the Internet and the limited jurisdiction of governments, it is nearly impossible for one country to solve these problems alone. This means that we need thoughtful leadership about how countries can work in partnership to address these problems. For example, countries can work together to develop international frameworks for intellectual property rights enforcement and best practices for domestic policies.

Policies do not need to be 100 percent enforceable to be effective. By using a layered approach that combines a variety of policy tools, countries can get closer to desired outcomes. This is not unique to Internet policy. Even countries that tightly control guns or drugs still have contraband, though typically at much lower levels than countries with more permissive laws. Each country must find the balance that is appropriate for its circumstances.

CONCLUSION

In short, 3D printing is a new technology that raises old policy questions. We should promote the technology while also ensuring that we have strong enforcement mechanisms and penalties, both domestically and internationally, to punish bad actors who abuse the technology by producing items that would be illegal regardless of how they were created. This will allow consumers to continue to reap the benefits of the technology while also protecting them from its potential harms.

ENDNOTES

1. As of May 15, 2013 two of Amazon's top-selling 3D printers were between $1,300 and $1,600. "3D Printers and Supplies," Amazon, May 15, 2013, http://www.amazon.com/b?ie=UTF8&node=6066126011.
2. "Liberator," DEFCAD, May 5, 2013, http://defcad.org/liberator/.
3. For a full list, see available downloads on DEFCAD at http://defcad.org/browse/.
4. Allison Terry, "Online blueprint for 3D gun violates export law, US says," The Christian Science Monitor, May 20, 2013, http://www.csmonitor.com/USA/USA-Update/2013/0510/Online-blueprint-for-3D-gun-violates-export-law-US-says.-Too-late-now.-video.
5. See, for example, Bernstein v. U.S. Department of Justice.
6. The 108th Congress passed H.R. 3348 in 2003 to reauthorize the ban on undetectable firearms. See http://beta.congress.gov/bill/108th-congress/house-bill/3348.
7. See H.R. 6704 in the 112th Congress and H.R. 1474 in the 113th Congress available at http://beta.congress.gov/bill/112th-congress/house-bill/6704 and http://beta.congress.gov/bill/113th-congress/house-bill/1474.
8. Steve Irsael, "Rep. Israel to Introduce Legislation to Prohibit 3-D Printed High-Capacity Magazines Along with Plastic Guns," January 16, 2013, http://israel.house.gov/index.php?option=com_content&task=view&id=1131&Itemid=7.
9. See Section P of 18 USC § 842 "Unlawful acts" available at http://www.law.cornell.edu/uscode/text/18/842.
10. Andy Greenberg, "Meet Steve Israel, The Congressman Who Wants To Ban 3D-Printed Guns," Forbes, January 18, 2013, http://www.forbes.com/sites/andygreenberg/2013/01/18/meet-steve-israel-the-congressman-who-wants-to-ban-3d-printable-guns-qa/.
11. "List of Printers Which Do or Do Not Display Tracking Dots," Electronic Frontier Foundation, n.d., https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots.
12. "Photoshop and CDS," Adobe.com, n.d., http://www.adobe.com/special/products/photoshop/cds.html.
13. Greenberg, "Meet Steve Israel."
14. "Thingiverse Terms of Use," Thingiverse, February 10, 2012, http://www.thingiverse.com/legal.
15. "Bomb Making Materials Awareness Program," Department of Homeland Security, n.d. http://www.dhs.gov/bomb-making-materials-awareness-program.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing input to this report: Rob Atkinson and Sue Wonder. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION, VISIT WWW.ITIF.ORG.