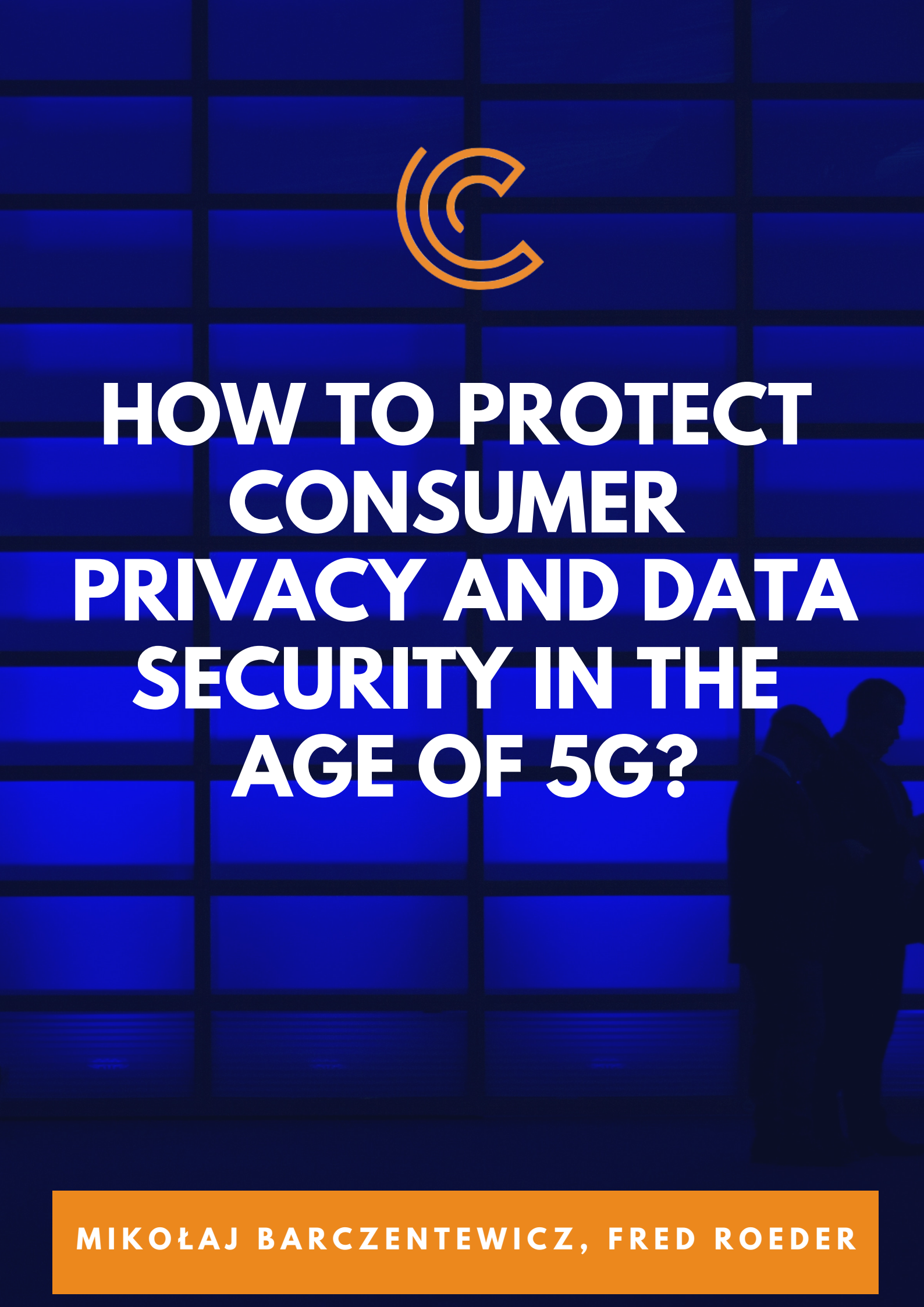

HOW TO PROTECT CONSUMER PRIVACY AND DATA SECURITY IN THE AGE OF 5G?

MIKOŁAJ BARCZENTEWICZ, FRED ROEDER

POLICY PRIMER

How to Protect Consumer Privacy and Data Security in the Age of 5G?

Consumer Choice Center – Policy Primer
By Mikołaj Barczentewicz and Fred Roeder

EXECUTIVE SUMMARY

This policy primer looks at current privacy risks for European consumers, how current legal rules are insufficient in protecting consumers' privacy in the age of 5G technologies, and what can be done by legal change and other policy measures to minimize consumers' exposure to data leaks and privacy breaches.

The scope of this analysis

- The key interests of consumers include not only low prices and quick adoption of valuable new technologies, but also privacy and data security.
- Government and private actions that undermine privacy and data security expose consumers to serious risk of significant harm (for example: financial crime, identity theft).
- Here, we focus on the problem of vulnerability of devices and software to malicious interference (data security). We are concerned with consumer products and services, as well as with electronic infrastructure.

Recommendations

- Consumers are best served by outcomes-focused and evidence-based policy. Blunt instruments like total bans based on country of origin should be seen as measures of last resort.
- We recommend using liability rules for operators and resellers of software and devices that expose consumers to risk of malicious and illegal interference. Personal liability of company directors may be worth considering.

- Liability standards should be assisted by security certification of software and devices (like proposed in the EU's "Cybersecurity Act"). The approach proposed by the EU Commission in its new recommendation on security of 5G networks is consistent with our recommendations.
- Promotion of strong encryption and of secure methods of authentication should be a significant part of the effort to safeguard consumer interests.

INTRODUCTION

Consumers are now exposed to significant risks because of their reliance on internet-connected software and devices. This reliance is only likely to grow with adoption of Internet of Things solutions and 5G networking.

We hear daily about new major cases of identity theft, financial crime, and other forms of attacks or malicious interference. Just recently, we learned about hackers taking over a software update server of one of the major hardware manufacturers, which allowed the attackers to install backdoors in thousands of computers.[1] What made it worse was that, according to press reports, the manufacturer did not react promptly when informed by security researchers, thus allowing attacks to continue. On the other hand, some governments aim to establish methods of user-unauthorised access to individual data (eg. by putting pressure on manufacturers to include backdoors in their devices), thus undermining security of digital products and services.

Such incidents are evidence that consumer data security, and thus also consumer privacy, are not being taken with sufficient seriousness. Some manufacturers and software developers tend to be mostly concerned about low prices and those aspects of their products that consumers immediately appreciate. However, they should be reminded that consumers also have strong interests in privacy and data security. We believe that there is a need for a smart policy response, that would incentivise market players to give sufficient weight to consumer data security but also achieve that goal without undue market distortions and limiting of consumer choice.

In this document, we focus on policy solutions for safeguarding consumer interests. We are not chiefly concerned here with what limitations should exist on public safety measures adopted by governments, but we do stress that any method that undermines data security is potentially liable to be exploited by any sufficiently motivated and

[1] Kim Zetter, 'Hackers Hijacked ASUS Software Updates to Install Backdoors on Thousands of Computers' (Motherboard, 25 March 2019) <https://motherboard.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers>

competent actor. In other words, backdoors installed by liberal democratic governments may be used by criminals or foreign governments.

POLICY SOLUTIONS

We present three potential solutions: liability, certification, and bans based on country of origin. They are not mutually exclusive – in principle they could all contribute to a comprehensive policy safeguarding consumer privacy and data security. They all come with some degree of downsides from the consumer perspective. We believe that **liability rules** are likely to offer the best balance between providing consumers with security and the cost of doing so. We are not convinced that bans based on country of origin should be implemented in the current context.

We welcome the new Recommendation of the EU Commission on Cybersecurity of 5G Networks as we believe that the approach adopted there is consistent with our recommendation and strikes the right balance between potential costs to consumers and the benefits consumers will have from increased data security.[2]

Some of the assumptions we made in offering the recommendations:

- There is no single silver bullet solution for safeguarding consumer privacy and data security. We need a mix of solutions and this mix will likely change over time.
- Healthy competition between legal jurisdictions and between private enterprises is the best mechanism for the discovery of the right tools. But all those working on solutions to issues of cybersecurity should give great weight to consumer interests.
- We do not take a position on what are the best technological solutions and thus embrace technology neutrality.
- Current legal rules (for example, Art. 32 GDPR[3]) do not provide sufficient clarity regarding the standard of supply chain security required.

LIABILITY

It is appropriate for the law to incentivise private enterprises (like manufacturers and importers of consumer devices, telecommunications operators) by adopting liability rules for using or reselling software or devices with vulnerabilities posing risks for consumer

[2] Commission Recommendation of 26 March 2019 on Cybersecurity of 5G Networks <http://europa.eu/rapid/press-release_IP-19-1832_en.htm?locale=en>.
[3] Art. 32 of the General Data Protection Regulation <https://gdpr.eu/article-32-security-of-processing/>.

privacy and data security. This should put pressure on non-European suppliers to adopt the security-by-design approach and to take pains to show that they have done so.
To some extent such liability rules (and relevant enforcement mechanisms) already exist given that data and communications security are already legal requirements on the level of EU law (for example, Art. 32 GDPR and Art. 16 of the NIS Directive[4]) and in national law.
Introduction of liability of manufacturers and importers of hardware for security vulnerabilities of products sold by them may require new legal rules.

We also recommend considering the option of personal liability of directors of companies which fail to address the risks discussed here.

Irrespective of whether general liability rules already exist, there is clearly a need for more specific authoritative guidance, or even new legal rules, on what is the appropriate standard of security for software and hardware. Both EU and national rules on electronic security tend to say not much more than that they require "appropriate measures" to be taken.

For example, the European Union Agency for Network and Information Security (ENISA), in its guidelines for SMEs says only that those who process personal data should ensure that "[h]ardware and software is obtained by trusted providers and following formal contractual procedures".[5] Given the concerns, for example, about supply chain attacks (like the one on software update servers we mentioned earlier) or even vulnerabilities intentionally inserted by manufacturers, this is far from being helpful and from providing an effective, legally enforceable standard.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC>
[5] ENISA, 'Guidelines for SMEs on the security of personal data processing' (December 2016), <https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing>

In solving the problem of insufficient clarity and effectiveness of the legal rules on data security (and thus of the standard of liability) the following should be taken into account:

- Technical standards should be as technology-neutral as possible. In particular, they should not require using specific products of services, because this will pose a barrier to market entry and technological development.
- Instead, the rules should be focused on outcomes and as general as possible while still providing sufficient guidance.
- Any standards should be possible to identify and adopt not just by the biggest market players, who can easily devote significant resources to compliance.

Those aims are hard to achieve through the means of general legal rules like GDPR. A certification scheme can be a good complementary solution.

CERTIFICATION OF SOFTWARE AND DEVICES

Liability for vulnerabilities could be excluded or diminished if the device or service was certified as secure. Some EU countries operate security certification schemes, but for the reasons given in the proposal of the EU Cybersecurity Act, this situation is suboptimal.[6] We welcome the certification scheme proposed in the EU Cybersecurity Act as it may – depending on how it is implemented – contribute significantly to safeguarding consumer data security. Naturally, we hope that the certification standards and procedures will be adequate given risks like manufacturer-created government backdoors.

[6] Proposal of a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477R(02)&qid=1553611735328&from=EN>.

We recommend that the certification schemes to be developed pursuant to the EU Cybersecurity Act require the following from products and services directed to consumers or handling consumer data:

- Encryption. End-to-end encryption of communications and encryption of data at rest significantly increase the level of protection against malicious interference. We believe that the less encryption adopted the higher should be the risk of liability (and the higher the penalties) for vulnerabilities or security breaches.
- Authentication. Consumers should always have an option to use exclusively (ie. without forced "backup" to less secure methods like SMS) the most secure method of authentication feasible for the given kind of product or service. For online services this should mean acceptance of the W3C WebAuthn standard (allowing logging in with hardware devices like Yubico YubiKey or Google Titan).

BANS BASED ON COUNTRY OF ORIGIN

There are reasons to believe that some governments put legal or extralegal pressure on private enterprises to include in their software or devices vulnerabilities that may be exploited either by government agents alone or with manufacturer's cooperation. This is being used as a justification for wholesale bans of products and services based on the country of origin. **Such bans are unlikely to be in consumer interest.**

A wholesale ban purportedly motivated by security concerns has the same effects as a trade restriction in the context of a trade war. The first victim of any trade war are the consumers of the country imposing tariffs and non-tariff barriers to trade. Unless there is no other workable solution and unless the evidence of a serious security risk is clear, this solution should not be adopted.

Consumers are best served by outcomes-focused and evidence-based policy. Blunt instruments like total bans based on country of origin should be seen as measures of the last resort.

About the Authors

Mikołaj Barczentewicz (@MBarczentewicz) is a Lecturer (Assistant Professor) at the University of Surrey School of Law, a Research Associate at the University of Oxford, and a Privacy Fellow at the Consumer Choice Center. He works on legal and ethical issues associated with new technologies. Mikołaj studied law and philosophy at the University of Oxford and at the University of Warsaw. Before his graduate studies at Oxford, he was a lawyer specialising in EU law and regulation in the Warsaw office of DZP, a leading law firm, and a law and policy expert at the FOR Foundation, a prominent Polish NGO founded by Professor Leszek Balcerowicz. Notably, Mikołaj lead a campaign for increasing the scope of freedom of information in Poland and, within that campaign, successfully sued the President of Poland in a high-profile cause litigation before the highest Polish courts.

Fred Roeder (@FredCyrusRoeder) is a German Health Economist and Managing Director of the Consumer Choice Center. He has been consulting governments, non profits, and the private sector on economic reforms in two dozen countries with a strong focus on emerging markets and post-communist countries. Besides healthcare his research areas are transportation, telecommunication, and digital technologies. He is a board member of several technology companies in Europe and North America and on advisory boards of several nonprofits and for profit corporations.

The CCC empowers consumers to raise their voice in media, the Internet, and on the streets and facilitates activism towards a more empowered consumer. Learning from the successes of its parent organization, Students For Liberty, the CCC will bring the struggle for consumer freedom to the next level.

The CCC represents consumers in over 100 countries across the globe. We monitor closely regulatory trends in Washington, Brussels, Geneva and other hotspots of regulation and inform and activate consumers to fight for #ConsumerChoice.

CONSUMER CHOICE CENTER

2221 S Clark St. 12th Floor Arlington, VA 22202, USA
info@consumerchoicecenter.org • consumerchoicecenter.org