5 February 2024

Dear Home Secretary,

We, the undersigned, write to express our concerns over the proposed changes to the UK's Investigatory Powers Act (IPA) notices regime. We write as individuals in our personal capacities who have devoted their careers and lives to building a safer, more reliable, and more inclusive Internet.

We are particularly concerned about two proposed changes:

1. The obligation for providers to notify the Secretary of State before making technical and other relevant changes to their products; and
2. The requirements for providers to refrain from making any technical changes to their services pending the review of the legality of a notice issued under the IPA.

If enacted, these proposals would have disastrous consequences for the security of users of services operating in the UK, by introducing bureaucratic hurdles that slow the development and deployment of security updates. They would orchestrate a situation in which the UK Government effectively directs how technology is built and maintained, significantly undermining user trust in the safety and security of services and products.

If combined with client-side scanning and surveillance powers in the Online Safety Act, these risks to security and trust are significantly exacerbated. Singly or as a whole, these proposals undermine the UK's ambitions to become a leader in technology development and investment. The effects of the proposals, once enacted, are unlikely to support the UK's National Cyber Strategy to be perceived as a "leading responsible and democratic cyber power."

Critically, these proposals would severely undermine privacy and security in two particular ways that are of grave concern – by delaying or slowing the release of security updates, and by threatening encryption.

Increased cybercrime risks

Internet users around the world – and those in the UK in particular – are facing an unprecedented and growing threat of cybercrime, which would be exacerbated by the interference with the timely deployment of security updates as proposed in amendments to the IPA.

These proposals could result in prohibiting, restricting, or delaying the deployment of software updates to address security vulnerabilities, since releasing those updates could constitute a change to the product, or could otherwise have a "negative impact" on the UK Government's ability to exercise its powers under the IPA. As the undersigned noted in a letter responding to a

French national security proposal addressing software vulnerabilities, “When significant vulnerabilities are discovered, the vendor’s top priority is to deploy a mitigation that prevents loss or damage, and to reduce risks until that mitigation is deployed. The period prior to the release of a mitigation is very dangerous for Internet users — there are no defenses to an attack.”

The National Crime Agency states on its website that criminals will exploit “security vulnerabilities in order to steal passwords, data or money directly,” and lists hacking of social media and emails as a leading threat vector. Similarly, the National Cyber Security Centre warned in its 2022 report that “the most significant threat facing citizens and small businesses continued to be from cyber crime” and that “the proliferation and commercial availability of cyber capabilities will expand the cyber security threat to the UK. In the future, malicious and disruptive cyber tools will be available to a wider range of state and non-state actors and will be deployed with greater frequency and with less predictability.”

These risks bear out in the statistics on real-world harm. While cybercrime is a global threat that is estimated to cost consumers and businesses £8.4 trillion GBP annually by 2025, the UK has been found to be at uniquely high risk with the density of UK internet users who fall victim to cybercriminals higher than anywhere else in the world. Official statistics released last April by the UK’s Department for Science, Innovation, & Technology show that in the UK alone, “26% of medium businesses, 37% of large businesses and 25% of high-income charities” fell victim to cybercrime in the previous 12 months. During that time, DSIT estimates that there were “approximately 2.39 million instances of cyber crime and approximately 49,000 instances of fraud” in the UK.

By interfering with the ability of operators to swiftly deploy software updates to patch vulnerabilities, these proposals would weaken security protections and exacerbate these risks, not only for the operators’ UK users, but for all their users worldwide.

Threats to Encryption

The proposals for operators to be required to notify the Secretary of State in advance of making any technical or other relevant changes, and to maintain the status quo or “freeze” their products’ capabilities while a review of an IPA notice is pending, pose a significant and direct threat to encryption.

The UK Government led a statement with allies, updated earlier this year, that simultaneously calls on providers to take steps that would break encryption to further law enforcement investigations while contradictorily affirming the importance of encryption and rightly acknowledging that it “plays a crucial role in protecting personal data, privacy, intellectual property, trade secrets and cyber security…serves a vital purpose in repressive states to protect journalists, human rights defenders and other vulnerable people…[and] is an existential anchor of trust in the digital world.”

Over the last several years, various ministries in the UK Government have acted on these calls and advanced technical and regulatory proposals to build encryption backdoors, such as with GCHQ's "ghost proposal", and a requirement for operators to develop technology to scan content in encrypted spaces, as the Online Safety Act threatens to do. Cryptographers and security and privacy experts have long been concerned that the notice authorities in the IPA could be used to force operators to build backdoors, or prevent them from deploying encryption by default on their services.

These "notify" and "freeze" proposals represent the UK Government's most recent attack on encryption. They seem tailored to achieve the goal that has, thus far, proven elusive to law enforcement: deter the provision and growing adoption of secure communications protected by end-to-end encryption, by ensuring that operators cannot deploy product updates to enable it by default for all users before the UK Government has the chance to prohibit or otherwise prevent it.

It is vital that governance of the IPA doesn't compromise the privacy or security of the Internet and its users, and the proposed regime should not weaken previously established legal and procedural safeguards in UK law. Any changes made by the UK Government will serve as a model for other countries and impact standards abroad.

We are deeply concerned that both of these proposals are anathema to the best interests of UK citizens and businesses and internet users everywhere, and contradict universally accepted security best practices.

We urge the Government to heed the concerns of security experts, industry, and wider civil society in finalising changes to the IPA.

Best regards,

Mallory Knodel, Chief Technologist, Center for Democracy and Technology and Member, Internet Architecture Board

Joseph Hall, PhD, Distinguished Technologist, Internet Society

Ryan Hurst, CEO, Peculiar Ventures

Tarah Wheeler, US/UK Fulbright Scholar in Cyber Security, CEO Red Queen Dynamics, & Senior Fellow for Global Cyber Policy at Council on Foreign Relations

Adam Shostack, Author Threat Modeling: Designing for Security

Chris Riley, Distinguished Research Fellow, Annenberg Public Policy Center, University of Pennsylvania

Wendy Seltzer, Principal Identity Architect, Tucows

Matthew Hodgson, CEO/CTO Element

Roya Ensafi, University of Michigan and founder of Censored Planet

Jon Callas, Distinguished Engineer at Zatik Security

Charles Mok, Research Scholar, Cyber Policy Center, Stanford University

Peter G. Neumann, Chief Scientist, SRI Computer Science Lab and Moderator, ACM Risks Forum

Jordi Domingo-Pascual. Internet Society Catalunya (ISOC-CAT)

Arne Möhle, cryptography expert, CEO Tutao GmbH

Matthias Pfau, cryptography expert, CEO Tutao GmbH

Christian de Larrinaga, Founder, ICT Systems

Susan Landau, Tufts University (for identification purposes only)

Carl E. Landwehr, consultant

Dr Marwan Fayed, SMIEEE, SMACM; Research Lead, Cloudflare; Research Visiting Professor, University of St Andrews; and Co-founder & Director, HUBS c.i.c.

L Jean Camp

Philip Zimmermann, Associate Professor Emeritus of cybersecurity, Delft University of Technology

Eugene H. Spafford, Ph.D., Professor, Purdue University and Executive Director Emeritus, CERIAS

Dr. Joseph Kiniry, Principal Scientist, Galois and CEO and Chief Scientist, Free & Fair

Sharon Polsky, MAPP — President, Privacy & Access Council of Canada

Sunoo Park, New York University

Nicholas Spooner, University of Warwick

Riana Pfefferkorn, Stanford Internet Observatory (for identification purposes only)

Dr Daniel R. Thomas, StrathCyber, University of Strathclyde

Sofía Celi, Brave