

Transforming Mobile Protection: Unlocking Digital Futures



Executive summary

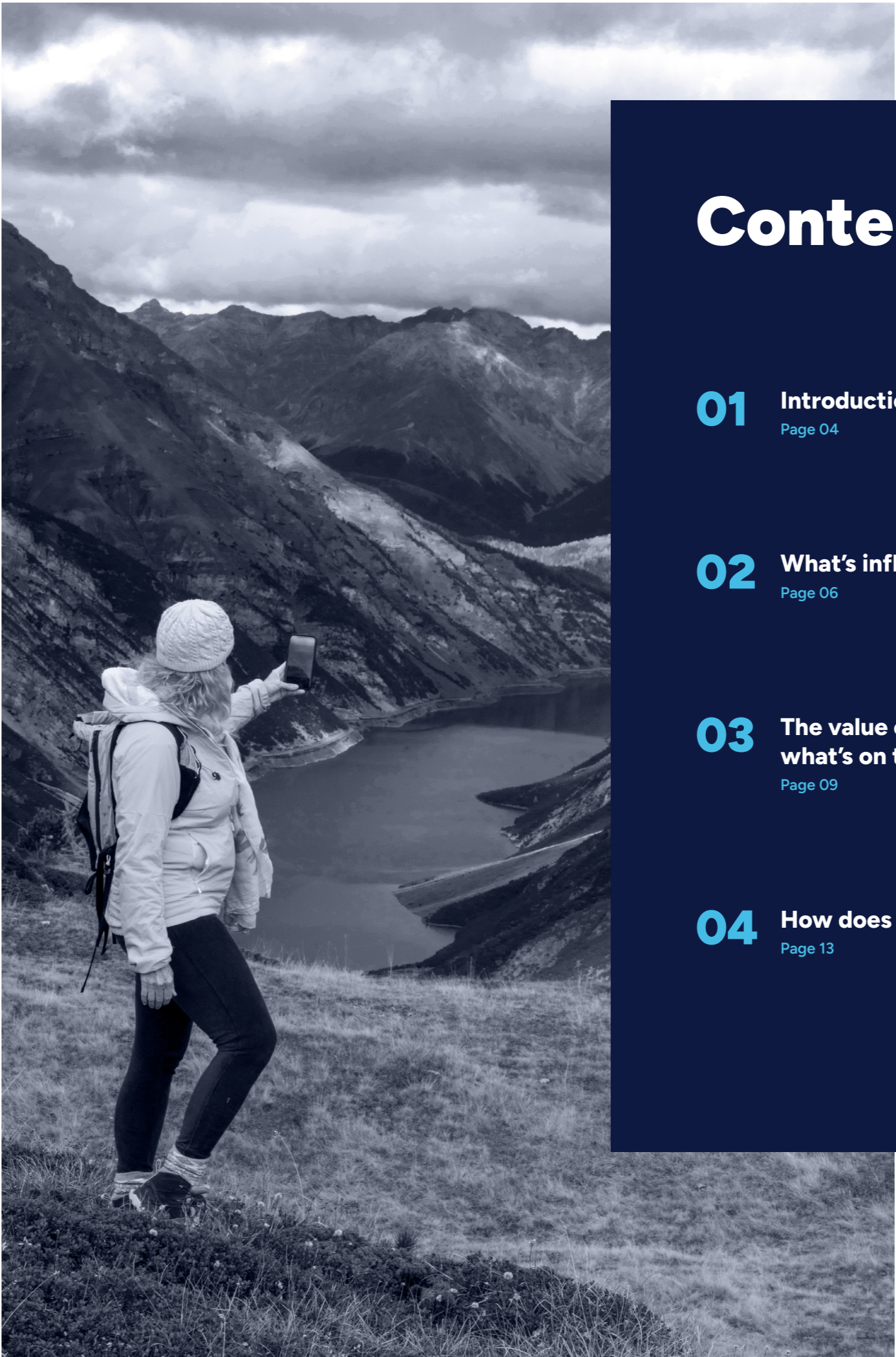
Mobile devices have become the ultimate enablers of modern life. Without them, we cannot function. The growing reliance on these devices, paired with consumers’ lack of adequate protection, presents a growing risk—one that will only escalate in the next five years.

By 2030, the mobile landscape will undergo a significant transformation. As our digital ecosystems become more complex, so too will the threats. To anticipate risks and protect consumers, the mobile ecosystem—including insurers, manufacturers, operators and regulators—must come together to develop holistic, adaptive solutions that put consumers at the heart of protection plans.

Key shifts on the horizon include:

- **The evolution of devices:** Over the last two decades, mobile devices have become more durable and advanced, with prices rising in line with improvements in capability and functionality. Looking ahead, what we consider a ‘mobile device’ today may take an entirely new form. Yet, while hardware has evolved, protection solutions have not kept pace.
- **A shift in ownership models:** The future will see device ownership allowing consumers to have the flexibility of owning the latest tech while re-integrating previous devices back into the ecosystem. At the same time, future protection will move seamlessly through the numerous devices one will own. Subscription models will help enable this shift.
- **The expansion of digital lives:** Mobile devices now store our entire digital identities—personal data, memories, and financial information. With AI advancements, they will become even more embedded in our lives, acting as intuitive personal assistants and even our ‘second brains’. This will come with risks that underpin the need for more advanced personal protection.
- **The future of protection:** Device protection will extend far beyond today’s insurance models. Insurers will collaborate with the mobile ecosystem to enable more intelligent, integrated safeguards; leveraging technologies that proactively monitor and protect users across their entire physical and digital footprint.

The future of mobile technology is one of near-limitless potential—but without the right protections in place, it is also one of vulnerability. The future therefore isn’t a product or plan, it’s a mindset and mission that integrates physical device protection with digital security, while creating sustainable device lifecycles in parallel.



Contents

- 01 Introduction
Page 04
- 02 What’s influencing the future?
Page 06
- 03 The value of our devices and what’s on them
Page 09
- 04 How does insurance need to evolve?
Page 13

01

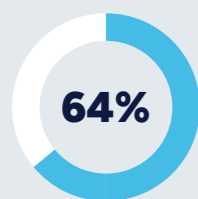
Introduction

When John Donne wrote ‘no man is an island’, he couldn’t have imagined a future where mobile devices could connect us to the entire world. But he did understand something fundamental about human nature—we crave connection, interaction, and belonging.

In the past few decades, innovators, engineers and visionaries have poured the brilliance of human ingenuity into creating technology that serves as an extension of this need. Today, our mobile devices are more than just a calling device; they are lifelines—central to how we work, socialise and express ourselves. No longer valued for just their hardware, they have become prized for the rich digital lives they enable.

According to [Wunderman Thompson](#), 76% of people now rely on technology for daily activities, and over half (52%) say it directly impacts their happiness. Research commissioned by SquareTrade found that 64% of UK consumers would feel disconnected from people in their lives and from being able to access critical information without their device.

As well as being integral to daily life, the way we own and interact with these devices is changing too. Consumers now depend on not just one, but three to five connected devices on average—from mobiles, tablets, laptops and a range of wearable smart devices. To make owning the latest and greatest tech possible, ownership models focused on accessibility and flexibility have emerged. In a multi-device world, where the seamless flow of data across



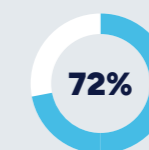
of UK consumers would feel disconnected from people and information without their device.



these devices is paramount, subscription and Device-as-a-Service (DaaS) ownership models will enable this shift, as consumers prioritise access over physical possession.

In many ways, our devices have become our modern homes—fulfilling essential needs like work, entertainment, connection, and access to our finances. Devices carry out everyday tasks. From buying a coffee to getting on public transport, they are needed to move through life. This is a relationship only set to deepen; Artificial Intelligence (AI) is already reshaping how we interact with technology, making our devices more intuitive, responsive—and even predictive—when it comes to our needs.

Of course, it’s not just the ability to conduct everyday tasks. Mobile devices also house people’s digital identities. Yet, consumers remain unaware—or perhaps in denial—of the risks posed by theft, cyber threats, and loss. Despite insuring our homes and cars, a significant protection gap exists for our devices. Nearly three quarters (72%) of UK consumers surveyed by SquareTrade report not having insurance on their mobile device. Many consumers realise the true cost of this lack of protection too late. Media accounts illustrate this all too well; when something goes wrong, victims describe not only the financial loss but the emotional devastation of losing personal memories and sensitive data.



of UK consumers surveyed by SquareTrade report **not having insurance** on their mobile device.

Further, many consumers struggle to navigate the complex web of options for protection. Should they opt for products offering cybersecurity, extended warranties, cloud backups, or even safeguards for social media and financial accounts? Understanding where protection begins and ends can be challenging, but the need for it has never been greater. People have become so reliant on their mobile devices that being without one can feel like severing a vital connection to the world, prompting an urgent need to have it back in their hands as soon as possible.

The rapid acceleration of technology and the increasing intelligence of our devices is creating a new protection reality—one that the entire mobile ecosystem must address. Bridging the gap between securing physical devices and protecting digital identities is no longer optional. It’s essential. As we look to the future, this will only become more complex as devices and technologies continue to evolve. Solutions will have to account for not only what devices are, but also how we interact with them, and how we own or subscribe to them.

So what can be done, and what will come next?

SquareTrade, an Allstate company, has partnered with strategic foresight consultancy The Future Laboratory to explore these issues in depth. This report features expert insights from Benjamin Hubert, founder of thought-leading design studio, LAYER, Chris Downs, founder and chief innovation officer at Normally, and Bryan Falchuk, founder and managing partner, Insurance Evolution Partners.







Second, by manufacturers who have consistently developed more affordable variants of high-end models, ensuring mass-market availability.

Over time, the capabilities of these budget-friendly smartphones eventually catch up to what premium mobile devices could do just a few product cycles ago.


Whichever device consumers opt for today, they have become the nerve centre of their daily lives. SquareTrade research finds that the majority of UK consumers rely on mobile devices for critical daily functions: 71% of consumers use their mobile devices to perform essential tasks (including navigation, communication and working). It's why, for most, being without a mobile device can feel like a crisis. They are intrinsic to modern human connection. [Nearly 40% of people interact more through screens than face-to-face](#), with Millennials and Gen Z




4.7 billion people own a mobile device



The majority of UK consumers **rely** on mobile devices for **critical daily functions**



The **mobile industry** alone is expected to contribute almost **\$6 trillion** to the global economy this year.



The average **upgrade cycle** reached an all time high of **43 months** in 2023.

02

What's influencing the future?

Devices will continue to evolve as well as how we use and own them

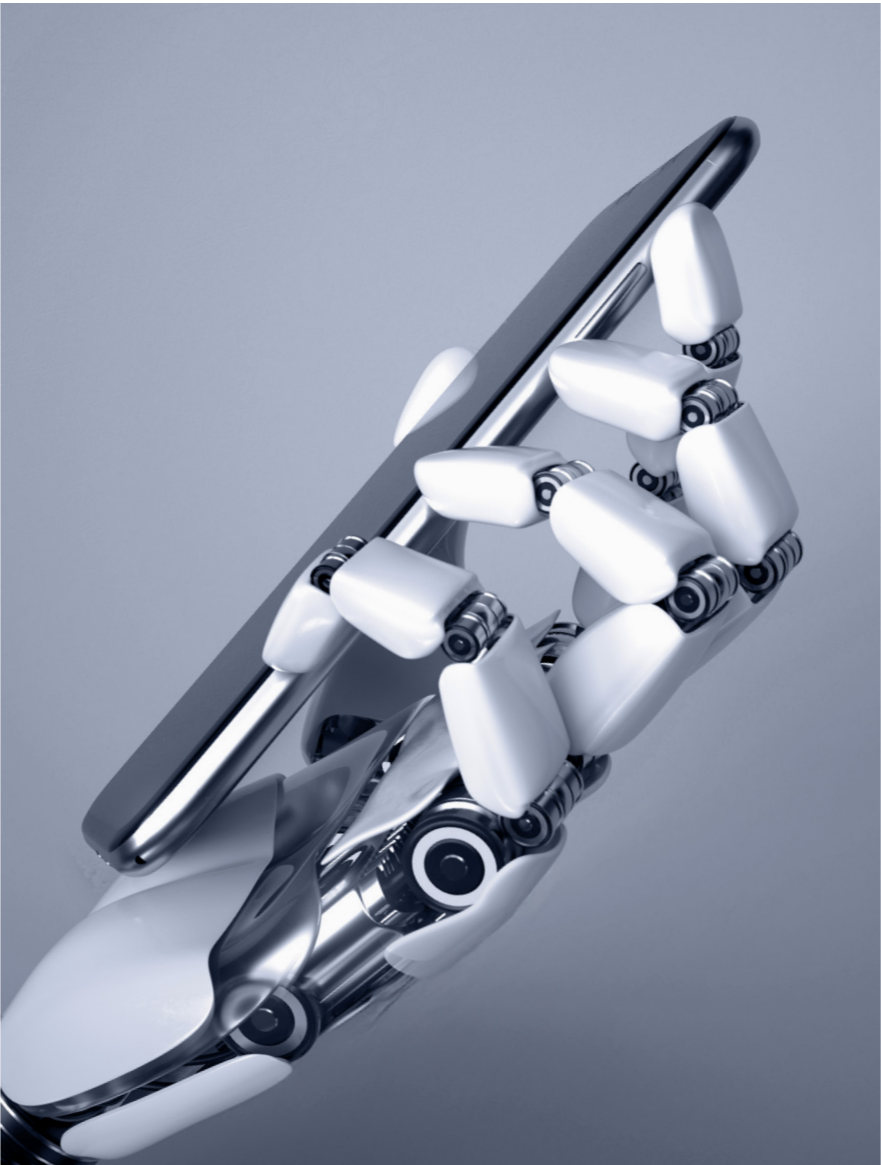
In just a few decades, mobile devices have evolved drastically to reshape how we connect with the world. In 1973, the Motorola DynaTAC 8000X, the first mobile phone, was a simple 'brick' phone used solely for calls. Fast forward to the mid-1990s, and Nokia's iconic ringtones became synonymous with mobile culture; games like 'Snake' started to hint at mobile entertainment's future. By the early 2000s, phones had gained basic data features like SMS and MMS, while Blackberry introduced email and messaging, transforming communication on the go.

Cut to the launch of the iPhone in 2007, which marked a turning point for mobile, introducing a touchscreen interface and a whole new world of user-friendly mobile apps.

Over time, these mobile devices have advanced, integrating capabilities like 48 mega-pixel cameras, that make high-end devices comparable to professional grade cameras. It's therefore unsurprising that premium mobile devices today can cost upwards of £1,000.

Yet, despite what can be a hefty price tag, mobile devices have become nearly ubiquitous with more than half the global population owning one today; the [GSMA puts the figure at 4.7billion](#). This widespread adoption has been driven by two key factors. First, by manufacturers and operators who introduced innovative financing models which made premium devices more accessible by allowing consumers to spread costs over time.

4.7 billion people now own a mobile device.



particularly likely to say devices help them foster meaningful relationships.

The brick has been replaced with sleek, pocket-sized computers, essential for connecting us with the world. We now rely on mobile devices to manage multiple aspects of our lives—from banking to navigation to learning a new language. The mobile industry alone is expected to contribute [almost \\$6 trillion](#) to the global economy this year.

Today's evolution of mobile technology can be defined by inherent dualities and tensions. On the one hand, we have devices more powerful and intelligent than ever, along with the emergence of innovations that hint at being revolutionary – Apple's Vision Pro for instance. Yet, many consumers remain reluctant to adopt them—not due to a lack of intrigue, but because they come with unjustifiable price tags for the average person and fail to meet the everyday wants and needs of most users.

As such, the mobile industry is reaching a state of equilibrium. The rapid technological leaps that once drove frequent upgrades have slowed, and today's mobile devices are not only more durable but meet the majority of consumers' needs for longer. As a result of this, consumers are holding onto their devices for longer, with the average upgrade cycle reaching an all time high of [43 months in 2023](#).

'The problem with the annual upgrade cycle is that the changes no longer feel material.' says Bryan Falchuk, Founder and Managing Partner of Insurance Evolution Partners. Analysts at Counterpoint also note that *'Consumers are holding on to their smartphones longer because upgrades often offer limited differentiation in features.'*

However, this lull in mobile innovation doesn't mean change isn't coming. While today's mobile devices may feature incremental rather than flashy upgrades, significant advancements in hardware durability are on the horizon. [CCS Insights](#) reports that, by 2028, nano-coating could enable our mobile screens to self-repair minor damage seamlessly.

Industry eyes are always on the next big thing, like the iPhone 20 years ago. Developments in AR headsets, smart glasses, implantable technology and self-repair features are all expected to define the next era of mobile. According to the Future Laboratory, by 2030 we will enter a new frontier—one where digital experiences are seamlessly integrated into the physical world.

Subscription becomes the mainstream

Over a lifetime, the average consumer is expected to own up to [20 mobile devices](#), equal to spending over £20,000. And that figure doesn't consider the growing number of connected devices people own today. From smartwatches and tablets to other wearables, the average person now owns between three to five connected devices. Each of these are subject to near-annual model upgrades that typically only introduce marginal improvements, often failing to justify high price tags.

As we edge toward the next game-changing innovation, one that might rival the first iPhone, one question looms large. How can consumers stay engaged with the latest the mobile industry has to offer without having to spend thousands of pounds every upgrade cycle?

A solution is already emerging, Device as a Service (DaaS). Mirroring trends seen in entertainment streaming and car leasing, this model shifts the focus from ownership to access. Over the next five years, these subscription models, like Apple's iPhone Upgrade Program, are set to grow in popularity. The model has especially struck a chord with tech enthusiasts who want a seamless path to getting their hands on the latest devices without the upfront cost, as well as opening up to a wider demographic of consumers who seek an upgrade—even if only for a better camera.

Subscription-based access will help to democratise the mobile market, just like long-term contracts once did, by removing financial barriers. Over time, this is likely to reshape consumer behaviour—turning hesitation to upgrade for minor mobile device enhancements into a new normal.



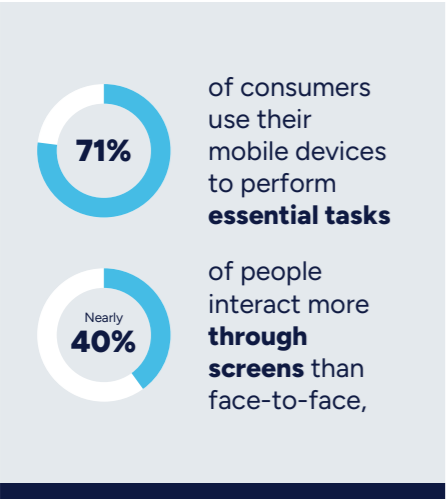
Furthermore, these DaaS models don't just benefit consumers, they also promote a more sustainable model by reintegrating the estimated [5-10 billion unused devices](#) worldwide back into the ecosystem. Their valuable components can be repurposed to reduce waste and support the circular economy, a shift accelerated by regulations like the EU ['Right to Repair'](#) directive.

By 2030, DaaS subscriptions are expected to dominate, propelled by repairability laws, consumer demand, and trade-in services that reduce emissions, conserve resources, and spread costs. This will empower consumers to own multiple devices tailored to their specific needs—whether that means accessing the latest technology with cutting-edge cameras or simply upgrading on their own terms, for as long as they choose.

For insurers, DaaS presents an opportunity to move beyond protecting one standalone device and instead provide coverage for an individual's entire digital ecosystem. At the same time, with an insurance bundle, consumers can experience the benefits of a holistic package that not only protects against device damage or loss but moves seamlessly between their devices.

As DaaS models mature, they will become more integrated with insurance protections. Consumers will benefit from more sophisticated and proactive protection that covers all of their devices, with improved safeguards in the event something goes wrong. This will be enabled by innovations like adaptive pricing and personalised coverage based on real-time risk analysis.

These services will help to reduce gaps in protection and will shift insurance from being reactive—covering losses—to proactive—automating protection and ensuring seamless access. For instance, by introducing much faster replacement options for consumers to ensure that, whatever happens, they always have access to a functioning and secure device.



03

The value of our devices and what's on them

Today, the physical loss of a device can trigger extreme panic. SquareTrade research found that UK consumers can't go more than an hour without their mobile device before anxiety sets in. This sense of attachment is especially pronounced among younger generations with 77% of 18–24 year-olds reporting they would immediately turn their pockets inside out and empty their bags in a frantic search of their device.

Disconnection anxiety and feelings of vulnerability are understandable. In today's world, mobile devices are essential for everyday life—from paying for goods to accessing public transport—so what happens if someone finds themselves left without one?

Practical resolutions will need to evolve, particularly to ensure that consumers aren't left in the dark in the event of loss, theft or worse. Today, insurers are already using AI to accelerate approvals, provide claim journey visibility, and reduce the time consumers are left without devices—and this use will only increase in the future.

However, reducing the time required for the resolution process will be an even greater priority for the insurers of tomorrow. While replacing lost or stolen devices has significantly improved in recent years—what once took weeks to resolve now takes just one business day—but there's still room for greater efficiency.

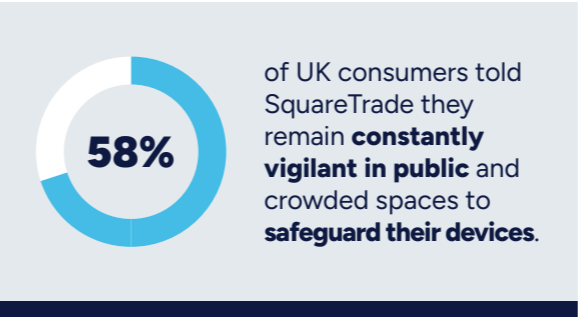
In the near future, AI will offer some answers by transforming claims processing by automating tasks. This will streamline operations, speed up payouts, and ensure



more accurate assessments, leading to fewer disputes and greater trust. By the end of the year, it's predicted that [30% of insurers](#) will automate underwriting processes, with early adopters set to reap the rewards.

Mobile devices, especially premium models, contain rare elements and high-value components, making them both expensive and difficult to extract. However, their value extends beyond just hardware; they now serve as vaults for entire digital identities—personal data, memories, and financial information. According to Juniper Research, digital wallets alone are expected to exceed [5.2 billion users](#) in 2026.

The anxiety of device loss can extend far beyond the inability to perform daily tasks. In the event of loss, our whole identity can be stolen from us. [A recent Deloitte Connected Consumer survey revealed that around one-third of consumers](#) would replace physical passports (34%) or driving licenses (33%) with mobile-integrated versions. This is a future already taking shape. In the UK, it's expected that, by the end of 2025, [a new law will allow](#)



A phone is stolen every six minutes in London.

people to use digital ID on their devices to prove their age when making age-restricted purchases.

The information contained on a mobile device is now more valuable than ever. This is translating to the global rise of mobile device thefts. The vast amount of personal data and information phones contain about their owners is extremely attractive to criminals. Across Europe, cities like Rome, Paris and Barcelona have become notorious hotspots for pickpocketing, with criminals now targeting mobile devices as aggressively as wallets. London, often said to have become the phone-snatching capital of Europe, has seen these types of thefts [surge by 150% year-on-year](#) (September 2024).

In London, a mobile device is stolen every six minutes, [while in the United States, 1.4 million devices were reported stolen in 2023 alone](#). Fraud is also another growing problem—whether related to theft, phishing or other scams—and is [estimated to cost mobile operators worldwide at least \\$10 billion a year, according to the GSMA](#).

Phone theft has become so widespread that nearly 60% of UK consumers told SquareTrade

they remain constantly vigilant in public and crowded spaces to safeguard their devices. However, when faced with crises like loss or theft, many overestimate the security of their mobile devices, unaware of how easily thieves can bypass protections. Biometric features such as Face ID may seem impenetrable, but criminals deploy tactics like waiting to grab mobile devices when unlocked in a victim's hand or observing as passwords are entered. Once appropriated, it is the richness of that individual's digital life—passwords stored in notes applications, access to social media accounts, and even photos of passport details—that allow thieves to break into bank accounts or commit identity fraud.

Falling victim to drained bank accounts, and online spending sprees, is one challenge. When it comes to the loss of personal data—heartfelt messages, videos of baby's first steps and family photos—the loss takes a far greater toll emotionally. [One victim told the BBC](#) how fraudsters took control of his mobile device, stole £21,000, and accessed sensitive business and personal records. Another shared how the last photos of a deceased family member were locked in their stolen device and that they'd 'do anything to have it back'.

When SquareTrade asked consumers about their primary concerns in the event of mobile device theft, the top four worries were potential risks to personal

The primary concerns consumers have in the event of mobile device theft;



Technology Solutions to Tackle Device and Data Protection in the Mid-Term-to-Long-Term

Our mobile devices are already learning more about us—tracking our habits, preferences and even basic biometrics. Over the next five years, and beyond, advancements in user behaviour and biometrics could provide new frontiers for security protections, enabling devices to recognise users based on their unique characteristics. By continuously monitoring these patterns, and understanding individual users, systems could detect anomalies in real-time, enabling proactive risk prevention across both personal and connected devices—fortifying security in the event of device theft or fraud.

Proactive protection

Devices of the future will work intuitively, learning user behavior and leveraging real-time monitoring to dynamically adjust permissions based on usage patterns. This proactive approach will detect and respond to potential threats before they escalate, ensuring both the device and personal data remain secure—all with minimal disruption to the user experience. Future devices will integrate

these capabilities to streamline recovery processes in the event of theft or loss—triggering a sequence of events that renders devices useless.

Protecting identity, with identity

Advances in biometrics will underpin proactive protection of the individual and their data. Personal data will be securely tied to proactive biological identifiers, including heartbeat rhythms, ensuring that information on devices remains encrypted and inaccessible without the rightful owner. In the event of theft or fraud attempts, devices will automatically lock down, making them useless to criminals.

As mobile devices evolve, so does consumer sentiment toward data privacy. Increasingly, people are willing to share personal information in exchange for greater personalisation, convenience, and security. [Jack Morton](#) research indicates that, since the rise of AI-driven platforms like ChatGPT, the percentage of consumers (aged 18-29) who prioritise keeping

their data private has dropped from 69% to 42%. A similar shift is seen in those aged 30-49, whose concerns fell from 64% to 49%, as they experience the benefits of AI-powered services.

This growing comfort with data-sharing presents an opportunity to reshape digital protection. The demand for intuitive, learning-based technology is rising, and security solutions built on a deep understanding of user behaviour will redefine how protection is delivered. As Chris Downs, Founder and Chief Innovation Officer of Normally, puts it: *'The conversation needs to be flipped. What if brands explained that they could use the same data and the same technology to actually help people—to look after them, protect them, and help them achieve what they want to achieve? There is potential to transform, not just how we use and think of protection, but how we access it too. AI can transform the process into an automated model, one where an intuitive assistant doesn't just recognise the issue but makes the claim for the user.'*

banking, loss of photos and memories, threats to their identity, and the loss of personal data. Today, the impact of losing a device goes far beyond the financial value of the hardware. This reflects the deep personal and emotional attachment consumers have to their devices, which have become central to their lives because of the vast amount of material and sentimental value they hold.

As Kevin Gillan, Managing Director, SquareTrade, explains, *'The industry today needs to do a better job of protecting the value of not just the device, but all that it unlocks and represents – both emotional and monetary. This includes safeguarding access to linked services*

and mitigating the challenges consumers face in recovery. The repercussions of attacks like these extend far beyond financial losses.'

The Unseen Vulnerability in Our Digital Lives

The growing disconnect between the increasing value placed on mobile devices and the risks they carry underscores a critical gap in consumer awareness, leaving us exposed to both financial and emotional harm. When a crisis strikes, consumers often feel

overwhelmed by the variety of plans required to fully secure their data and identity, such as device and cyber insurance, cloud backups, and warranties from different providers. It can be an overwhelming burden to action numerous claims when recovering from the loss of a device. While device insurance is common, fewer consumers consider protecting their data and digital vulnerabilities. Many don't fully understand the risks of cybercrime or assume their existing insurance covers cyber risks, which it often does not.

For those who are insured, confusion can arise from overlapping coverage. For example, if a mobile device is stolen and used for banking fraud, the device insurer may replace the phone, while the bank may offer fraud compensation. However, determining who is responsible for the full loss can be unclear, as it involves both device and cyber issues.

A significant number of UK consumers (43%), surveyed by SquareTrade, find navigating insurance policies too confusing, feeling unsure about which policies they should have and which they shouldn't.

Additionally, almost 30% report being undecided, further reflecting the high levels of uncertainty surrounding current protection plans.

Only 18% of respondents claim to fully understand the differences between their insurance policies and what's covered - whether for home, mobile device, or banking.

As Benjamin Hubert, founder of thought-leading design studio, LAYER puts it: *'We live in an age where technology is accelerating very quickly, but our understanding of it is not accelerating at the same rate. It's both a responsibility and a question for the mobile ecosystem. How do you deliver protection for the frontier, cutting, bleeding edge of technology and its changing implications on our daily lives?'*

The Emerging AI Landscape

AI integration is also pushing this evolution further and at a greater pace. Devices as mainstream as the iPhone are already becoming vehicles for AI-powered lifestyles. They're evolving to help us to write, express ourselves and get things done, all by their intrinsic understanding of us as individuals.

As AI evolves into ambient computing and extended reality (XR), our devices are poised to transition from handheld devices to wearables and, eventually, seamlessly integrated technologies. Our mobile devices will no longer respond to commands—they will anticipate our needs, filter distractions, prioritise tasks and even compose messages in our tone and style before we start to type a word. Personalised AI agents will assist in real-time, translating languages, summarising conversations and providing instant insights tailored to our surroundings. Further ahead, AI could enable implanted devices that allow us to interact with digital environments through thought alone, fundamentally redefining our relationship with our mobile devices.

Advancements in technology are paving the way for personal devices to function as second brains, enabling memory recall, contextual computing, and dynamic digital archiving. Innovations in spatial computing and layered realities, such as the Memory Machines project by Dutch research firm Modem, hint at a future where devices enable immersive memory documentation, allowing individuals to relive past experiences in vivid detail.

Just 18% of people understand what their device insurance covers and what it doesn't.

Beyond augmenting memory, devices could evolve into gateways to Artificial General Intelligence. Future devices might instantly archive users' data—photos, emails, and more—into searchable memory hubs, revolutionising how we create, curate, and protect our digital lives; essentially becoming our 'second brains'.

For Benjamin Hubert, Founder of design studio LAYER, the consumer appetite for embedded tech is clear: *'There's an innate desire for personal devices to be as integrated and as invisible as possible. The future is so embedded, and technology is so embedded as a part of people, that in the future, the separation will almost not be there at all.'*

Consumer appetite for future mobile device technologies is palpable, especially among younger generations. SquareTrade research found that 62% of Millennials and Gen Z (18-34 year olds) are excited about making use of future potential use-cases leveraging technologies like AI.

However, in a future of near-limitless potential, without the right protections in place, we risk leaving ourselves painfully vulnerable. A new wave of security challenges will emerge with increased AI usage. This will see malicious actors using AI to craft ever-more sophisticated phishing attacks, with deepfakes making it increasingly difficult to detect scams. The surge in global cybercrime reflects this growing danger and is expected to [reach \\$10.5 trillion USD in losses this year](#), up from \$3 billion USD in 2015.

Vulnerable groups, such as the elderly and young people, face unique risks when navigating online spaces. Older individuals often struggle to identify sophisticated AI-driven scams, making them easy targets for cybercriminals. Meanwhile, children and young adults are increasingly susceptible to social engineering and phishing schemes on social media. Alarmingly, this marks a reversal of traditional safety norms: today's children are often safer in the physical world than in the digital one. While Generation X earned the label "latchkey kids" for their unsupervised freedom to roam around their neighbourhoods, modern children are heavily protected offline yet allowed unprecedented freedom online—a paradox with potentially serious consequences.

As mobile devices shift from status symbols, valued for their hardware alone, to vehicles allowing us to access our rich digital lives, the risks of not protecting them adequately will extend far beyond lost or damaged hardware. In the emerging landscape, the consequences of things like data breaches, identity theft, or access to personal or business information becomes more severe—and will demand a more comprehensive approach to what device insurance covers.



04

How does insurance need to evolve?

By 2030, mobile protection will be reshaped by the evolving ways consumers own and use their devices and what they value on them. As next-generation technologies converge with greater industry collaboration, a dynamic and preventative ecosystem will emerge—one that not only safeguards devices but individuals' data by proactively adapting to consumer needs. This transformation will depend on stronger data sharing and policies that keep pace with technological advancements.

Karl Wiley, CEO, SquareTrade explains; *'We're moving into an era where protection is something that is inseparable from having a device. Soon, consumers won't want, or expect to have, separate device protections.'*

As we move towards 2030, the possibilities of what the future of the mobile industry may look like, are vast. From the nature of what a mobile device is—whether it remains

a physical object or evolves into something more abstract like an implant or glasses—to how we interact with these devices, the industry will change.

Technologies like AI could unlock new possibilities that range from immersive experiences to devices functioning as our second brains. But as we look to the future, one



thing is clear. Our mobile devices, and by extension, the insurance industry, will be shaped by consumer wants and needs.

Over the past few decades, innovation in the industry has been shaped by one central question: What can our devices do for us?

As consumers, and society, become more interconnected, and as mobile-enabled technologies become increasingly central to our lives, so too does the need to protect them.

To meet the needs of tomorrow's consumers, insurers, manufacturers and regulators must act now, working together to create solutions adapted to people's rich digital lives across all the devices they use. This demands innovation and a collective commitment to embedding security, convenience, and sustainability into every aspect of device ownership.

Collaboration is needed to create consumer-centric protection plans. Working toward a more protected future will require insurers to address this urgent need to not only protect the hardware but protect individuals' identities and their data, which will only continue to be spread across the multiple devices they will own.



What's coming next?

- By 2028, self-healing screens powered by advanced nano-coatings will make cracked displays a thing of the past, transforming durability and slashing repair demand.
- With 30% of insurers projected to automate underwriting by 2025, those investing early in AI will secure a decisive competitive advantage.
- By 2030, underwriting will be reshaped by AI into a real-time, predictive process, offering tailored policies and near-instant risk evaluation.
- AI will be a double-edged sword, enhancing real-time threat defense by proactively monitoring app usage while also, as the [NCSC](#) (part of the GCHQ spy agency) warns, "almost certainly" driving a surge in cyber-attacks within the next two years. Expect a high-stakes arms race over the next two years.
- By 2030, circular economy models will dominate, propelled by repairability regulations and trade-in services that cut CO₂ emissions and reduce costs. Deloitte's survey reveals that 62% of consumers are ready to pay more for sustainable products, highlighting rising demand for circular solutions.
- By 2030, integrated Protection Hubs will emerge, as insurers partner with mobile operators and manufacturers to consolidate device management, protection, cybersecurity, and support into a unified dashboard, enhancing user experience and simplifying claims and recovery.
- Beyond 2030, mobile devices will transition from handheld instruments to wearables and implanted technologies, acting as second brains that enable memory recall, contextual computing, and dynamic digital archiving.
- Insurers will roll out all-in-one protection plans, offering seamless, end-to-end coverage—from screen repairs to data recovery—redefining the mobile ownership experience.

Solutions must be seamless and flexible, ensuring uninterrupted coverage as users transition between devices.

The future of mobile protection is not just about offering coverage; it's about a mindset shift that combines security, convenience, and accessibility with proactive, adaptive protection that moves with consumers across devices, platforms, and emerging digital environments.



Report methodology

This report was commissioned by SquareTrade and developed by The Future Laboratory, a globally renowned futures consultancy. The Future Laboratory used a combination of social and cultural macro research, validated by SquareTrade stakeholders, external experts, and quantitative research, to provide a comprehensive exploration of how personal device protection might evolve by 2030. At the core of The Future Laboratory's work is a proprietary foresight methodology, underpinned by an understanding of fundamental human needs and global drivers. The consultancy uses mixed methods to gather cultural and consumer insights, which inform its trend hypotheses. Central to this approach is The Future Laboratory's in-house 'Foresight Research System' - a dynamic, internal database continuously updated by a multidisciplinary team of analysts, researchers, and strategists. To enhance the research, The Future Laboratory conducted interviews with experts specialising in emerging technologies, technology design, and insurance. These discussions were critical in validating the findings, interrogating the research, and identifying key themes related to the future of personal devices. The research was further supported by a consumer survey conducted by OnePoll, which gathered insights from 2,500 UK-based smartphone owners aged 18 and older. The survey fieldwork took place between January 6 and January 20, 2025.

**square
trade®**