



Securys

Hospify 

Data privacy in the era of digital health

How covid-19 has changed the data landscape and what you should do to stay ahead of the game.

Privacy made practical[®]



Interactive
eBook

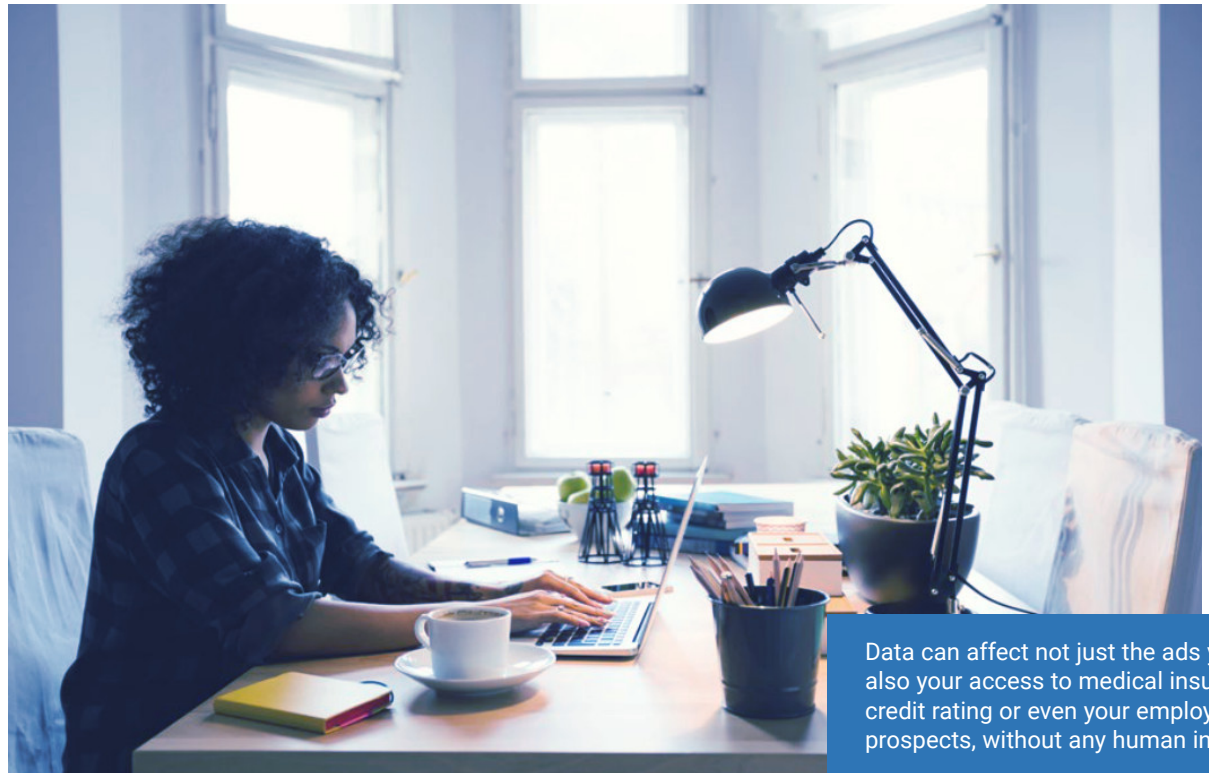
About this eBook

As technological innovations and the digitisation of health services bring improvements to healthcare and drive efficiencies in the organisations that provide it, the correct handling of sensitive patient data, otherwise known as “data hygiene”, has become a practice as vital as that of physical hygiene.

Given the context of a broader consumer digital industry dominated by free-to-use services that exploit personal data for commercial ends, both clinicians and patients need to understand the importance of securing their data, and to learn how to do this in ways that are both practical and allow for the best possible patient outcomes.

In this eBook we take a look at the regulations that define appropriate approaches to handling patient identifiable data (PID) and the extraordinary impact that the response to the covid-19 pandemic has had on the health and care sector.

Ever mindful of both the needs of the individual patient and the pressures brought to bear by the tech giants, we also take a look at the Information Governance (IG) challenges involved in doing this, along with the opportunities facing those affected by digital health - a rapidly growing industry that at some point soon will touch us all.



Data can affect not just the ads you see but also your access to medical insurance, your credit rating or even your employment prospects, without any human intervention.

Sponsors and involvement

This eBook is brought to you by Hospify and Securys.



Hospify is a simple & secure way of sharing sensitive & confidential health information between individuals, teams & communities.

Our free messaging app can be downloaded from the app stores; the team messaging platform (the Hospify Hub and Web App) can be purchased by hospitals, surgeries and other healthcare institutions.

Together, the Hospify Mobile App, Hub & Web App combine the best of consumer tools like WhatsApp, LinkedIn and Slack, in a manner that's appropriate for use in health.



hospify



info@hospify.com



@HospifyApp



www.hospify.com



Securys is a specialist data privacy consultancy with a difference.

We're not a law firm, but we employ lawyers.

We're not a cyber-security business but our staff qualifications include CISSP and CISA.

We're not selling a one-size-fits-all tech product, but we've built proprietary tools and techniques that work with the class-leading GRC products to simplify and streamline the hardest tasks in assuring privacy.

Above all, our relentless focus is on practical operational delivery of effective data privacy for all stakeholders.



securys-limited



hello@securys.co.uk



@SecurysUK



www.securys.co.uk

Interacting with our eBook

This interactive eBook has been designed to include links and references outside of this document. Typically these include online articles, videos and general pieces of information to help support a given topic. All links are clearly highlighted, either as buttons or as hyperlinked text within the main content.

Contents

Why does privacy matter?	5
I've got nothing to hide	6
Data regulations in the time of COVID	7
The regulator's approach	8
How it should work	10
The Securys take on privacy	12
The era of digital healthcare has arrived	13
The Hospify story	14
The future	16
Takeaway	17

Why does privacy matter?

It's about trust and safety for everyone – professionals and patients alike.

Healthcare is about trust

Medicine and social care can only function if patients and clients feel able to speak freely and fully about their circumstances, their symptoms and their needs. We trust our physicians and other care providers with our deepest secrets. They hold our lives in their hands and see us at our most vulnerable. Anything that threatens that trust threatens the whole web of care that is carefully woven around us.

Healthcare is about sharing

Very few cases can be addressed by a single practitioner. Even the simplest tests or most straightforward prescriptions mean data must be shared. For complex cases this is multiplied many times over, with dozens of professionals needing to have the right information at the right time in order to serve the person in their care. Yet every act of sharing also carries risk. Risk of breach; risk of misdirection; risk of error; risk of failure. Lack of information can kill, as can the wrong

information. But too much information, or information in the wrong hands, can also do harm. Privacy works to find the balance where what is necessary is available, only for as long as it is required, to those who need it.

Healthcare has boundaries

The connection between patient and care-provider is an intimate one. It can be hard for patients to remember that their doctors also have private lives; indeed, it can be hard for doctors to remember that at times they themselves may become patients. Privacy helps us maintain a healthy separation between public work and private life; it protects all parties.

Healthcare is driven by data

Few disciplines generate as much data as healthcare; fewer still have so many different uses for those data, uses beyond the care of a single patient which may eventually benefit millions or billions of people. But not only do

those potential benefits not outweigh the interests of the individual patient, misuse of these data may do actual damage. Privacy provides discipline and limits on sharing, imposes the need to anonymise and encrypt, and requires transparency about use and location to prevent that possible harm while permitting the pursuit of the greater good.

Healthcare is about people

Patients, carers, physicians, practitioners, administrators, support staff – all of us are involved in health in some way. All of us stand to benefit from the system working well and all of us stand to be harmed when it doesn't. While we seek always to drive technology forward we must remember that behind the apps and drugs and machines and treatments are humans who have complex needs and great vulnerability. Privacy is a reminder and a protector of that fundamental human frailty, the same frailty which the healthcare system is also fundamentally designed to protect.

I've got nothing to hide

Not too bothered about your health data being accessible by companies? Think again!

PID (patient identifiable information) is any health information that can be linked to any identifiable individual, which it generally can be **if it is not properly anonymised**.

But why should those used to being targeted by digital advertising, managing their public personas on social media and maintaining the public profile that comes with modern digital life be so concerned about their PID being divulged to companies and other organisations?

PID is subject to stringent regulation designed to keep it private, secure and out of the hands of those who would exploit it for commercial gain. The temporary relaxation of those regulations during the covid-19 crisis risks this confidential information ending up in the hands of companies with commercial imperative to exploit it.

Consider also the potential impact of metadata in communicating over channels such as WhatsApp. Even if the message content is not being analysed by Facebook (the owner of WhatsApp), the existence of the exchange, the identities of both parties and contingent information such as time, date, frequency and length are all recorded, in most cases along with geolocation and technical data, about the devices being used.

This information all then contributes to Facebook's profiles of its users, profiles that are then used to target commercial services and advertising. And with social media data increasingly playing a role in machine-learning

intermediated decision making including, for example, those behind the setting of insurance premiums and credit ratings, any inference that can be drawn from communication between a clinician and a patient could have a material impact on outcomes in those areas.

For instance it's likely that positive and negative covid-19 diagnosis messages will have different lengths, allowing anyone with access to the metadata to infer the covid status of recipients. This issue is not fully reflected in the regulatory advice around the handling of these data.

Information in context

Imagine that you are asked to have a remote consultation during lockdown with a specialist to whom your GP has referred you, conducted using an encrypted social media messaging app.

Although fit and healthy, you have a family history of a particular form of cancer. You wanted confirmation when you should next have a checkup and for any precautionary advice. No other information is shared.

The holding company which owns the messaging app holds the record that you have spoken with an oncologist. It sells the ability to search this data.

Years later and still healthy you apply for medical insurance. The insurance company runs a search on you and finds an association with oncology. The insurers decline to offer insurance or do so at a vastly inflated premium.

Data regulations in the time of COVID

Relaxed enforcement of regulations has given the NHS confidence to quickly deploy new technology, but at a cost.

At the peak of the covid-19 crisis in the UK in early April 2020 there were [over 1,000 covid-related deaths per day](#), an [estimated 90,000 people](#) in the UK were carrying the virus, hospitals were inundated with coronavirus patients, NHS England was preparing seven critical care Nightingale Hospitals, the Glasgow's SEC Centre was being transformed into the NHS Louisa Jordan, and NHS Wales was preparing the Millennium Stadium and a series of regional locations as pandemic treatment centres. By mid April nearly half of UK doctors were [suffering burnout](#), depression or anxiety.

To help meet the enormous challenges that the covid-19 crisis presented and to keep a country functioning in lockdown and with social distancing, extraordinary measures were required. Beyond the largest population lockdown in British history and a financial package which would ultimately support over [nine million people](#) on furlough it was clear that rapid innovation beyond

physical and regulatory measures would be needed to stem the spread of the disease.

Introducing new and readily available technological solutions to workflows was seen as vital to support and coordinate activity during the crisis. But introducing technology platforms in the healthcare sector is not a rapid process. Lengthy purchasing procedures must be navigated, stringent compliance regulations must be met, and an army of end users must be won over to a new way of working.

The crisis presented an opportunity for innovation, forcing upon institutions and staff new ways of working. New purchasing frameworks were hurried through and freely available collaboration and [communication platforms were considered](#).

At the same time clinicians that had been using popular mobile apps such as WhatsApp and

Skype in their personal lives were feeling increasingly compelled to start using them in the workplace new platforms in the workplace - indeed, according to NHS Digital's own figures, around 600,000 of them were already doing that before covid even arrived.

Anticipating this, the Information Commissioner's Office (ICO) relaxed its regulatory approach, (see our chapter, [The Regulators' Approach](#)). However, this gave rise to the possibility that data, including private patient medical data, could be held outside the European Union and UK, beyond the reach of the regulators, and by companies intent on using personal data for commercial ends.



It's not all about what can go wrong. Privacy can also be a positive selling point.

The regulator's approach

The Information Commissioner's Office (ICO) intervention was swift. On March 12th - the same day that the UK's Chief Medical Officer raised the covid-19 risk level from medium to high - the ICO published a statement recognising the extraordinary nature of events and the overwhelming interest of public safety.

"The ICO is a reasonable and pragmatic regulator, one that does not operate in isolation from matters of serious public concern," [the statement](#) read. "Regarding compliance with data protection, we will take into account the compelling public interest in the current health emergency. The safety and security of the public remains our primary concern."

Considering that the Premier League had not yet been suspended (that was announced the following day) and England was not to be subjected to full lockdown regulations for a further two weeks, this relaxation of bureaucratic measures might have seemed precipitate.

Within a week NHSX followed the ICO's statement with [advice that made allowances](#) for healthcare professionals to use messaging tools such as Microsoft's Skype, Facebook's WhatsApp and



Apple's FaceTime in the course of carrying out their duties.

Clinicians reading the headlines that followed might have been forgiven for thinking that all NHS Information Governance and GDPR restrictions had been lifted, and that they were now free to discuss patient cases with colleagues on WhatsApp.

However, when the guidance was examined more

closely, it became clear that it contained certain caveats. Not only was permission not extended to the storage of patient identifiable information (PID) using these consumer tools and the restriction of its transmission to instances of absolute necessity, but there was also an insistence that strong passwords and other data protection measures were used. In fact, it appears that the exemptions were really only designed to allow clinicians to use consumer video conferencing solutions, which do not store data by default, rather than messaging solutions like WhatsApp and Facebook Messenger.

The NHSX advice also deferred to the [ICO Working from Home Guidelines](#) which specifically say that: "if you need to share PID with others then choose NHSMail, a secure messaging app or online document sharing system."

So while the regulators did relax advice and enforcement during the pandemic in the interests of the greater public good, they did not give *carte blanche* to the storage or transmission of PID using consumer tools on unsecured devices.

The misinterpretation of this advice goes beyond individual clinicians. No less than Matt Hancock, the Secretary of State for Health and Social Care, tweeted that GDPR “has a clause excepting work in the overwhelming public interest,” without providing any clarifying detail.

In fact, the actual provision (as defined in Article 9 of the GDPR and in Schedule 1 Part 1 of the UK Data Protection Act 2018) is for work by public bodies empowered by enactment for specific purposes and does not apply to private organisations such as employers.

Unfortunately the regulator has chosen not to carry out any visible enforcement action or to challenge the government’s position, which has allowed these misinterpretations to propagate.

Online and offline you are your data, so protect it

Patient data shared on WhatsApp and other messaging services ends up in the hands of organisations with a commercial imperative to exploit that data.

The fact is that data breaches are never temporary. Once data are made available on the internet, they will remain there forever.

If these data belong to you, they will very likely be used to profile you by machine learning algorithms, profiles that are in turn sold on to advertisers, government agencies, political

pressure groups, insurers and all kinds of other bodies. Even if the content is itself encrypted, the meta-data around it - who you’re communicating with, how often, and what kinds of communication - can be almost as revealing about your behaviour as what you’re actually saying.

In turn, therefore, the data can affect not just the ads you’re likely to see while browsing but your access to medical insurance, your credit rating or even your employment prospects without any human intervention.

With social media data playing an increasing role in machine-learning-intermediated decision making... any inference drawn from communication between a clinician and a patient could have a material impact on people’s lives.

How it should work

Greater clarity from the regulators and authorities is needed to ensure that following the extraordinary response to the covid-19 pandemic everyone knows where they stand.

While almost all organisations have seen their capacity greatly reduced during the lockdown, the ICO and other leaders urgently need to return to business as usual, in as much as that is [possible in our post-covid world](#). Not only should guidelines be clear, but it must be clear to organisations and the public that they will be enforced.

It is not just for bureaucratic - or even legal - reasons that this clarity of regulation and visibility of enforcement is needed. If we are to recover from this still very present pandemic, public confidence in the handling of data is vital. Already we have seen widespread concern over the use of the data collected by the track and trace app and this greatly affects the efficacy of any measures that can be put in place. If they are to hand over their data, members of the public must be confident that these data will be handled

carefully, securely and used only for the purposes stated.

The EU's General Data Protection Regulation of 2017 created a clear set of international standards for governments and businesses to follow when handling data of all kinds, PID included. This regulation is now incorporated into and implemented by national legislation through Europe (in the UK's case by the Data Protection Act 2018), and these standards have also travelled further afield, with many countries on other continents, such as South America, using the GDPR as a template for overhauling their own data protection laws.

Health practitioners are well aware of these regulations and will have received extensive training on them - annual data protection training is now a requirement throughout the NHS, for

example. Healthcare professionals should know their Information Governance (IG) and should be able to put into practice what they have learned.

Fortunately the technology is also now there to support them in this. Even if working remotely or without the provision of a business laptop or phone, it is possible to operate in a compliant way using NHS-approved apps such as Hospify.

The framework is there, it simply needs to be followed; the technology is available, it simply needs to be used.

Secure applications...

- Minimise the data that is stored and do not store data unnecessarily for protracted periods.
- Are protected by a password/PIN or a biometric log in, and do not display sensitive data in homescreen notifications.
- Keep all data encrypted both at rest and in transit.
- Do not allow data to be backed up without the right information governance and authorisation in place.
- Comply with relevant regulations such as GDPR and the UK Data Protection Act 2018.
- Are registered with the Information Commissioner's Office.
- Have industry certifications such as ISO27001:2017 and Cyber Essentials in place.
- Comply with industry standards such as NHS Data Security Protection toolkit and Clinical Safety Risk Assessment.



The Securys take on privacy

What if privacy wasn't just a compliance issue? What if it didn't only sit within risk? What if it wasn't something organisations merely look to tick off?

[At Securys we do things differently, and we work with clients such as Hospify who share our view of privacy](#)

We're all about keeping things practical; we don't just give advice on law and regulation, we design and implement privacy programmes that work with our clients' businesses. Our senior professionals stay hands-on involved in project work, not just at the initial pitch, and our internal training programme and focus on staff privacy certifications mean that all of our consultants are privacy experts.

[We're not the department of saying no](#)

Whether your organisation is for-profit or non-profit, you have clear goals and ambitions. You don't want privacy to be a blocker and neither do we. Our job is to help you achieve those goals while preserving and protecting privacy for all of your stakeholders. We take the time to understand your operation and collaborate with

your managers to make sure privacy is working with and for them, not against them. Our senior team has extensive prior commercial and non-profit experience – we know about running businesses as well as advising them.

[We want you to benefit from good privacy](#)

We work in privacy because we believe that privacy is not just a fundamental human right but also a positive contributor to business success. We look for clients that share this belief; we want to help you do well by being good. Consumers, employees and business partners increasingly look to work with or buy from good corporate citizens. They want brands whose purpose and ethics align with their own brand values. Privacy done well is more than box-ticking: it's a competitive advantage.

We've committed to a year-long research project to put hard figures against the proposition that privacy done well builds trust with all

stakeholders, including customers and employees, and that this trust is repaid in everything from lower talent acquisition costs through higher investor valuations to better net promoter scores. Keep an eye on our [Privacy made Positive hub](#) for regular updates on our research and get involved!



Millennials in particular have demonstrated that their buying decisions, their employment decisions and their voting decisions are linked to value and purpose, not just price, salary and self-interest.

The era of digital healthcare has arrived

It's already a bit of a cliché to say that several years' worth of digital innovation and adoption have taken place in the NHS in the last two or three months, but that's because it's pretty much true.

During the covid-19 crisis NHS stakeholders have been willing - and permitted - to fast-track new ideas and take a few risks in a way that hasn't really been possible before. As a result the gates of the health service have been opened to a lot of digital tools that have been around for a while and waiting for their moment.

And it's not just clinicians that have changed their attitudes; patients have too. There's been a huge rise in the proportion of people now happy to consult with their doctor using phone, messaging or video, when even as recently as six months ago that felt like a fairly risky and even slightly suspect thing to do.

Because the digital tools in question are now reasonably mature, whole areas of the industry have been able to switch to new ways of

working relatively seamlessly. Now that this is happening, very few people seem to want to go back to the old ways of working regardless of what happens when the pandemic is finally over.

The advantages for both patient and clinician in terms of time saved, travel costs reduced and infection risks lowered or eliminated are just so apparent to all involved that it seems extremely unlikely that digital health techniques won't be a permanent and major part of the health landscape from now on. They have downsides too, of course, and are not appropriate for every eventuality, but deployed correctly they can make sure that physical presence is reserved for situations where it is genuinely required and can thus add more value than it does at present, when systemic pressures mean that face-to-face interactions are often unduly rushed.

“Microsoft has seen two years of digital transformation in two months.” Satya Nadella

Digital communication is a key part of all this. Poor, out-dated and heavily-siloed communication has hampered the NHS for years. Hospify is devoted to trying to bring better, simpler comms to all parties involved in health – whether patient, carer or clinician – while retaining the highest standards of data guardianship and regulatory compliance, and while keeping true to the service's guiding principle of being free at the point of use. We're absolutely convinced this can be done and indeed are now well on our way to doing it. If covid-19 has achieved one positive thing it has been to show how quickly tools like ours can spread when the need arises, as well as showing how great a need is there.

The Hospify story

Hospify was started to give clinicians a better way to communicate than the phones, faxes and bleeps that the health sector has relied upon for decades but which have become an increasing source of inefficiency and frustration.

The inspiration for Hospify came when Neville Dastur, a vascular surgeon at Frimley Park, was operating on a patient and couldn't get hold of a key colleague whose assistance he needed because the contact list had been removed from the theatre wall.

Neville linked up with James Flint, a technology journalist and entrepreneur with deep experience of building media platforms, and together they set out to develop a reliable and secure way for doctors and patients to connect, discuss and share sensitive information.

With the support of the Bethnal Green Ventures, Wayra Velocity Health and Kent Surrey Sussex Digital Health accelerators, Hospify launched the first iteration of its health network platform just in time for the advent of GDPR, beginning with a messaging app that was specifically engineered at the back end to prioritise privacy, security and

information governance while still giving users an intuitive and simple experience similar to that offered by popular consumer services.

Thanks to its scrupulous attention to data compliance, Hospify obtained ISO27001 and Cyber Essentials certification, met the exacting standards of the NHS Data Security Protection



Data privacy during and after the pandemic

Listen to how Securys and Llewellyn Consulting think lockdown will change the way we work going forward.

toolkit and Clinical Safety Risk Assessment, and became the first general messaging platform to be approved by NHS Digital for inclusion in the official NHS Apps Library.

At Hospify we are passionate about protecting sensitive patient information while offering a great service to the clinicians who work with that information to deliver the best outcomes for their patients. We're also very grateful to have had the opportunity to support the NHS, wider healthcare services and patients during the covid-19 global health emergency. Our health network has expanded four-fold during the pandemic and our scalability has been tested as our messaging volumes increased more than 100-fold.

Hospify remains the only messaging app that is approved by the NHS for use by both clinicians and patients. It is a simple, secure and compliant way to handle, store and disseminate sensitive patient-identifiable information.

Hospify has quadrupled its user-base since the UK lockdown started and has seen its messaging volumes increase more than 100-fold.



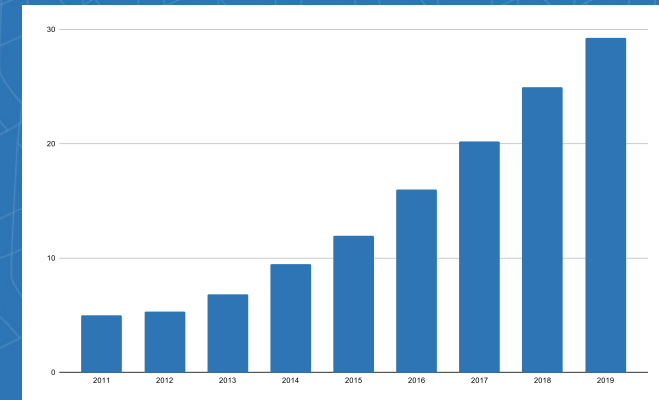
How much does Facebook make per user?

Facebook, which also owns WhatsApp and Instagram, provides free-to-use social media platforms. Income is generated principally from targeted advertising.

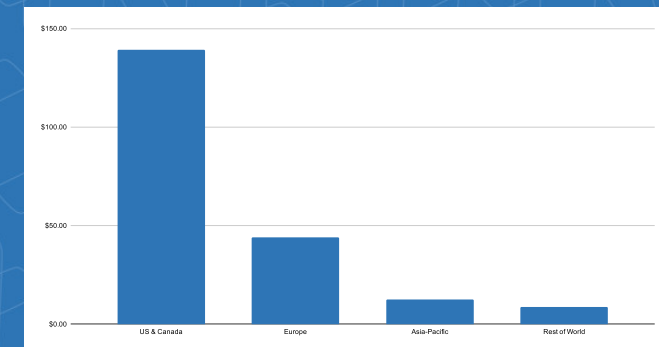
According to their Earnings Report, Facebook made \$29.25 per user last year.

However, US & Canada users represent a much higher level of income, around \$139.35 per annum, whereas in Europe it is \$44.14, \$12.63 in Asia Pacific and \$8.74 for the Rest of the World.

Source: data taken directly from Facebook financial accounts.



Average Revenue Per User (US Dollars)



Average Revenue Per User by Region (US Dollars)

The future

“It's really not about health versus economics. Public health is the road to economic recovery.”

In a recent [interview with the Telegraph](#) Dr Tom Frieden, the Director of the US Centres for Disease Control and Prevention under Barack Obama, spoke candidly about the handling of the covid-19 crisis and the route to recovery. He points out that new infectious disease outbreaks are inevitable and navigating covid-19 and any future outbreaks successfully will be dependent on governments following public health advice.

If the rate of economic recovery is dependent on public health policy and measures then trust in the health system will be crucial to the health of a nation and its economy. Individuals should know that sensitive data is being handled securely and in their best interests.

Follow the money

Businesses too can [benefit from showing leadership in Information Governance](#). We know that people value things they care about, and

that this influences their behaviour. Today's consumers are looking beyond price when choosing products and businesses that can meet their needs will find themselves pulling ahead of the competition.

Tensions on the global stage also represent risks to the handling and misuse of personal information and will increasingly focus attention on the curation and exploitation of data. Questions over Russian interference in US elections and the Brexit referendum, high profile hacking, social media scandals and growing tensions in trade and the protection of IP, particularly between the US and China, are all bringing data security to the fore in news and public debate.

It is unwise to try to predict the future, especially in such uncertain times, but data are - and will continue to be - a valuable commodity. Our decisions around the handling of sensitive data will surely therefore help shape the economic, corporate and political landscape to come.

When anonymous data isn't anonymous

There have been a number of well-publicised studies in which identities have been restored to seemingly anonymous data.

In October 2009 at [the University of Texas](#), two computer scientists, Vitaly Shmatikov and Arvind Narayanan, showed that anonymised data from Twitter, Flickr and Netflix can be re-identified. By overlaying anonymised data that is sold to advertisers or otherwise made publicly available with known identified data, it is possible to enrich many data sets with personal identities.

“When companies and organisations that have your data say they protect your privacy, what do they actually mean?” asks Vitaly Shmatikov.

“They normally think they can share the data if they just anonymise it by removing the names and any identifying information, such as Social Security numbers and email addresses, and that there is no privacy issue.”

Shmatikov and Narayanan were able to demonstrate that even with a data set modified with additional privacy measures, such as random errors and altered timestamps, it was still possible to re-identify individuals.

[“In practice, it's very easy to re-attach a name to anonymous data,”](#) says Shmatikov.

Ofcom's Online Nation 2020

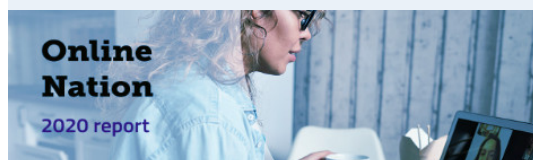
How search engines earn their revenue

In Ofcom's latest summary of online usage, 73% of internet users say they are confident in their ability to control their personal data online, but only half (53%) of adults recognised that the main source of income for search engines is advertising. That was lower again for YouTube, where just 43% identified the main revenue channel as advertising.

Concern over data usage

Almost half of internet users (45%) said that they were not happy for their personal information to be collected by companies under any circumstances (up by 6% YOY).

While WhatsApp is now being used almost as much as SMS on a daily basis (40% of users), new specialist services such as [Messenger Kids](#) (youth and families) and [Hospify](#) (healthcare) have seen significant growth.



Takeaway

At the end of the day, the person best placed to take care of your - and your clients' - privacy is you.

Privacy is the responsibility of all of us, and even if we don't much care to bother with it on our own account, when we're shouldering that responsibility on behalf of others it is at best unprofessional and at worst irresponsible - and potentially even criminal - not to pay it proper heed.

Laws and regulations set the terms of engagement and help define our culture, but as we've seen throughout this eBook regulators do not have the power or the reach to police everyone effectively - nor would we want them to, as that would create privacy issues in itself!

We've seen the damage that lack of digital privacy can do, both to individual liberties and to social and democratic processes. We have to start to realise that the digital is no longer a separate realm, it's a part of our everyday experience, as much as walking down the street or taking the bus to work.

Just as we dress our bodies appropriately in a suit or overalls or scrubs or a uniform to better do our jobs, so we need to learn to dress our minds appropriately for work as well. We now know enough about the way digital platforms work to understand that it is simply not acceptable to use Facebook or WhatsApp or Snapchat or TikTok to talk to clients if their data are likely to be sensitive in any way at all.

Digital is now part of our public space, seamlessly integrated with the physical world when we're both at work and play.

A surgeon uses a scalpel not a bread knife; and wears scrubs, not swimming trunks. The right tools for the job are out there, in both the real and virtual worlds. Find them, use them - and advertise your choice because you know that it reflects well back on you. And leave the Speedos for the pool.





Hospify 

Securys



1st Floor, Block C, The Wharf
Manchester Road, Burnley
BB11 1JT, Lancashire

E info@hospify.com
W www.hospify.com

 [hospify](#)
 [@HospifyApp](#)

161-165 Farringdon Road
London
EC1R 3AL

T 0800 193 8700
E hello@securys.co.uk
W www.securys.co.uk

 [securys-limited](#)
 [@SecurysUK](#)