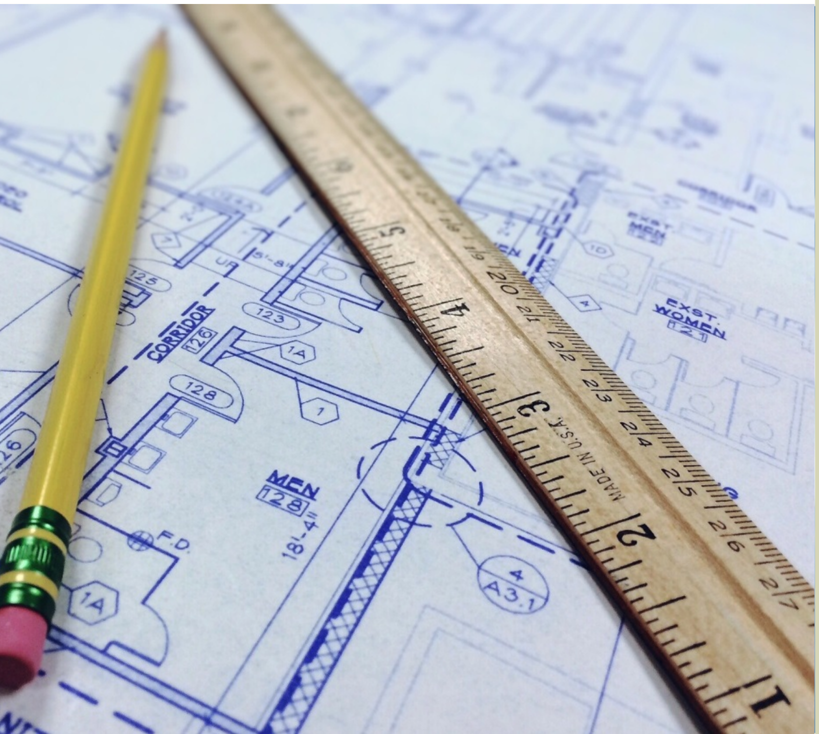
Stratecast | FROST & SULLIVAN

11 August 2017

Our Detailed Privacy Blueprint:

What All Parties Should Be Doing Right Now to Protect the People and Organizations They Care About

Stratecast Analysis by
Jeff Cotrupe



Stratecast Perspectives and Insight for Executives (SPIE)
Volume 17, Number 28

Our Detailed Privacy Blueprint:

What All Parties Should Be Doing Right Now to Protect the People and Organizations They Care About

Introduction[1]

We have seen the future of IT, and it is big data. The IT shop of the future has a big data lake on the front end, which it constantly updates with the freshest available data, making that data accessible to business and technical users alike, to help optimize all areas of the business. As we note in virtually every report we write, and in every Growth Consulting engagement we undertake for clients, organizations are beginning to reap a welcome range of quantified business, operational, and technical benefits from leveraging big data.

A serious threat exists, however, to the growth, or even continued use, of big data: the loss of privacy, which is already generating actions that limit data usage. The private sector has thus far failed to get privacy right. As a result, the public sector is increasingly stepping into the fray with regulations designed to force companies to respect consumer privacy, and punish those that do not comply. Privacy regulations can shut down most of the benefits of big data, leaving organizations ill-equipped to compete in the global economy. Nowhere is that more true than in the EU. The EU's General Data Protection Regulation (GDPR), intended to protect the privacy of EU citizens, threatens the viability of business initiatives in the region—all of which depend on data.

This SPIE completes our current four-part analysis of privacy.[2] The report briefly touches on conditions and factors posing threats to privacy; then, moves into the main thrust of the piece: analyzing each recommendation outlined in our Privacy Blueprint.

An Array of Privacy Threats Could Shut Down Big Data

Every invasion of privacy increases the likelihood of government intervention in the use of data. This section gives a brief overview of privacy issues and threats.

Private Sector Failure to Reach Privacy Consensus Leads to Public Sector Overreach

The GDPR is the most comprehensive set of privacy protections ever enacted into law. Its provisions on Right to be Forgotten; Data Portability; Data on Ethnicity/Affiliations; Increased Territorial Scope; Data Protection Officers, and onerous penalties, also may collectively prevent companies from legitimately using data by imposing various measures that appear impractical and

[1] In preparing this report, Stratecast conducted interviews with representatives of 10 organizations. Please note that the insights and opinions expressed in this assessment are those of Stratecast, and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

[2] For comprehensive analysis of privacy threats; a broad range of potential solutions; and our detailed assessment of the GDPR, we recommend Stratecast, *We Have Seen the Future of IT, and it is Big Data: Part 1 - Will IoT Privacy Issues Steal the Future?* (BDA 5-01, June 2017), available here; Stratecast, *We Have Seen the Future of IT, and it is Big Data: Part 2 - A Blueprint for Privacy, in the IoT and Everywhere* (BDA 5-02, June 2017), available here; and Stratecast, *Big Data is in Big Trouble, Starting in the EU: How the EU's GDPR Threatens to Destroy Big Data Initiatives and Business Opportunities, in the EU and Elsewhere* (BDA 5-03, July 2017), available here.

potentially cost-prohibitive. The EU passed the GDPR into law in 2016, and will begin enforcing it in May 2018.[3]

The IoT is Creating Big Opportunities—and a New Wave of Privacy Threats

Privacy concerns were already top-of-mind for many. Then, along came the Internet of Things (IoT), which vastly expands privacy threats. More than 12 billion devices were connected to the IoT in 2016, projected to grow to more than 45 billion devices by 2020.[4] One unintended consequence is that those deploying IoT are thrusting ordinary objects, never designed with the Internet in mind, onto the front lines of privacy.

No Standard Exists to Guide Manufacturers on Building Privacy into Products

The IoT is an abstract collection of products with no paradigm for implementation and use. Standards specify how devices communicate, but there are too many standards, each implementing different provisions. The result is a series of walled gardens that, at best, may be individually trustworthy, but do not necessarily work well together.

Some Regulations Appear More Focused on Protecting Providers than Consumers

Healthcare providers sometimes hide behind the Health Insurance Portability and Accountability Act of 1996 (HIPAA) when it comes to things like obtaining records from a hospital stay. However, hidden in HIPAA is a provision that prevents patients from suing healthcare providers who violate privacy. Providers fought for this as a way to avoid costly lawsuits; legislators knuckled under so the legislation would pass.[5]

The Explosion of Information and Technology Leaves Consumers Grasping at Air

Consumers, whose data is the object of all privacy discussion, face information overload, and new privacy threats hitting closer to home every day. It would take nearly a month of 24-hour days for the average consumer to read the legalese thrust at them to obtain applications and services in a typical year.[6]

[3] For our detailed analysis of the GDPR, we recommend Stratecast, *Big Data is in Big Trouble, Starting in the EU: How the EU's GDPR Threatens to Destroy Big Data Initiatives and Business Opportunities, in the EU and Elsewhere* (BDA 5-03, July 2017), available here.

[4] Frost & Sullivan's IoT Universe practice, *Internet of Things 2.0: Predictive Intelligence,* available here

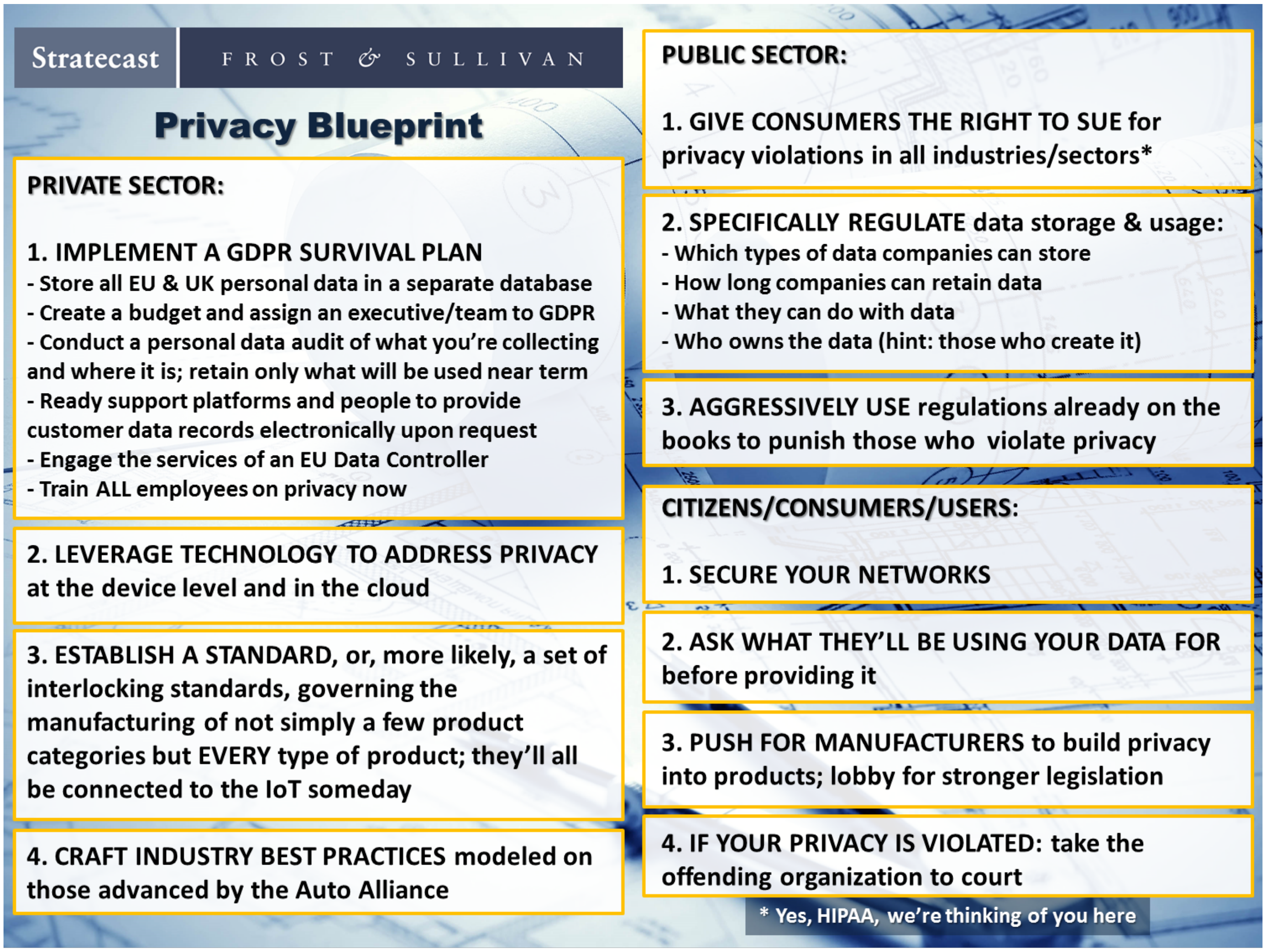
[5] The author recently experienced this first-hand, having to run an electronic gauntlet trying to retrieve copies of his own records from a recent hospital visit. To add privacy violation to injury, the hospital in question claims it cannot find forms containing his personal medical information that the hospital demanded from him that day.

[6] The Atlantic, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days,* available here

A Privacy Blueprint: What All Parties Need to Do Right Now

Privacy is at risk; which means that the world's ability to use big data is also at risk. All hope is not lost, however. Figure 1 presents our recommendations in Stratecast's Privacy Blueprint.

Figure 1: Stratecast's Privacy Blueprint



Stratecast | FROST & SULLIVAN

Privacy Blueprint

PRIVATE SECTOR:

1. IMPLEMENT A GDPR SURVIVAL PLAN
- Store all EU & UK personal data in a separate database
- Create a budget and assign an executive/team to GDPR
- Conduct a personal data audit of what you're collecting and where it is; retain only what will be used near term
- Ready support platforms and people to provide customer data records electronically upon request
- Engage the services of an EU Data Controller
- Train ALL employees on privacy now

2. LEVERAGE TECHNOLOGY TO ADDRESS PRIVACY at the device level and in the cloud

3. ESTABLISH A STANDARD, or, more likely, a set of interlocking standards, governing the manufacturing of not simply a few product categories but EVERY type of product; they'll all be connected to the IoT someday

4. CRAFT INDUSTRY BEST PRACTICES modeled on those advanced by the Auto Alliance

PUBLIC SECTOR:

1. GIVE CONSUMERS THE RIGHT TO SUE for privacy violations in all industries/sectors*

2. SPECIFICALLY REGULATE data storage & usage:
- Which types of data companies can store
- How long companies can retain data
- What they can do with data
- Who owns the data (hint: those who create it)

3. AGGRESSIVELY USE regulations already on the books to punish those who violate privacy

CITIZENS/CONSUMERS/USERS:

1. SECURE YOUR NETWORKS

2. ASK WHAT THEY'LL BE USING YOUR DATA FOR before providing it

3. PUSH FOR MANUFACTURERS to build privacy into products; lobby for stronger legislation

4. IF YOUR PRIVACY IS VIOLATED: take the offending organization to court

* Yes, HIPAA, we're thinking of you here

Source: Stratecast | Frost & Sullivan

As can be seen in the diagram, privacy does not involve just one party or area. Not only will public and private organizations be required to address privacy concerns; individuals, too, are called upon to think in terms of which actions they should be taking with regard to privacy—including closely considering which data they wish to maintain as private. The following sections analyze and support the recommendations outlined in Figure 1.

Action Items for the Private Sector

Obviously, a major player in the privacy game is the private sector. Data has become the lifeblood of most businesses and industries, so the private sector has the most to lose if data use is restricted. Our action items for the private sector are as follows:

1. Implement our GDPR Survival Plan.

We believe the GDPR may have a chilling effect on business; but it will also challenge organizations to be at the top of their game data-wise, which is not a bad thing. Here is our GDPR Survival Plan:

- Practice "EU Partitioning": store personal data on citizens of the EU and UK[7] in a separate database, physically located in the EU. Cloud hosting providers, on a standalone basis and in partnership with BDA providers, offer storage options supporting EU Partitioning.
- Create a budget, and assign an executive or team to be accountable for ensuring that you are ready for GDPR enforcement.
- Conduct an audit: determine exactly what personal data (as defined in the GDPR) you are currently collecting, where you are storing it, and how long you are retaining it. If you find that you are retaining any personal data that you cannot justify for essential and imminent business purposes, destroy it. This must apply to all personal data held on citizens of the EU—but your organization would do well to consider implementing at least some of these best practices with regard to all personal data, EU and otherwise.
- Make sure customer support people and platforms are ready to quickly provide customer data records electronically. If your platforms do not support rapidly providing data to customers upon request, update or replace platforms. Update customer records with email and other contact points so your people can quickly transmit data upon request.
- Engage a local partner. If you do not have an employee in the EU, something of a cottage industry is springing up for (human) EU Data Controllers, and you need to locate one now.
- Train every employee on privacy. Your company's posture on privacy is only as strong as your weakest link.

In addition, if your partners are not GDPR-compliant, they could drag you into violations. Talk with partners to ensure they are GDPR-compliant, or actively working toward compliance.

2. Address privacy at the device level and in the cloud.

The argument that equipping all devices with privacy protection 'costs too much' falls flat when manufacturers, solutions providers, and clients are already adding cost and going well outside normal processes to embed sensors, intelligence, and networking in devices to connect them to the IoT. Industry has a number of options here:

- Limit personal data collection. Follow the lead of one retail analytics provider that uses IoT-connected in-store cameras in its solutions. This provider uses software, implemented via the cloud, to make its cameras blur images; as a result, the system can recognize 'a shopper' passed the camera, but cannot determine shopper identities. Other providers achieve the

[7] Which is implementing GDPR, despite Brexit

same types of results by adding privacy protection functions to computer chips embedded in the connected devices.

- Leverage communications service providers (CSPs). CSPs are already involved in IoT deployments to provide connectivity between smart devices and the IoT core or cloud. Leverage their heritage of protecting subscriber data to ensure the privacy of user data in the cloud.

Addressing privacy in both areas will give the entire data ecosystem a head start.

3. Establish a standard or set of interlocking standards governing the manufacture and development of all components of the IoT.

It will be challenging to establish a standard governing all aspects of the IoT: devices, sensors, networking, software, computing platforms, communications and security protocols, and more. That does not excuse industry from doing everything it can in this regard. The standard(s) should apply to any device currently manufactured—and forward-compatible to devices that do not exist today. Someday, every manufactured project may, or likely will, be connected to the IoT. The world must be prepared when that day comes. As to which governing body should spearhead this effort, we suggest these potential leaders:

- Federal Trade Commission (FTC) and equivalents in other nations
- Internet of Things Privacy Forum (IoTPF) or Future of Privacy Forum (FPF)
- US-based National Association of Manufacturers, working with manufacturing consortiums in other world regions
- Stratecast | Frost & Sullivan

Given the potentially chilling effects on big data if not resolved, internal discussions are underway at Stratecast about the prospect of leading such an initiative.

4. Craft industry best practices modeled on those advanced by the Auto Alliance.

Privacy concerns began boiling over more than a decade ago, driven by consumer watchdog groups and legislators, about the use of personal data in advertising and retail. (Notwithstanding that these parties appeared unaware that every move made online since about 2007 has been tracked exactly the same way.) The Digital Advertising Alliance (DAA) and Future of Privacy Forum responded with best practices for online advertising, mobile marketing, and use of retail and location analytics:[8]

- DAA – Self-Regulatory Principles for Online Behavioral Advertising
- DAA – Self-Regulatory Principles for Multi-Site Data
- DAA – Application of Self-Regulatory Principles to the Mobile Environment
- Future of Privacy Forum – Mobile Location Analytics (MLA) Code of Conduct

[8] Digital Advertising Alliance, available here; and Future of Privacy Forum, available here

Consumer privacy concerns are now growing with regard to vehicles, given the amount of data that drivers and passengers—especially when connected to vehicle-based Wi-Fi or Bluetooth networks—may be sharing with dealers, manufacturers, and other parties in the Internet of Cars (IoC). Also, as mentioned previously in this section, since vehicles are high-priced manufactured items compared to many others, automakers are less likely to use cost as a reason to balk at building in privacy protections. That is reflected in the action of the Alliance of Automobile Manufacturers (the Auto Alliance), representing 70% of US car and light truck sales, which has developed a code of conduct regarding privacy that its members agree to live by.[9]

Other industries should follow the lead of the Auto Alliance, as well as the DAA and the Future of Privacy Forum, and adopt codes of conduct for their members.

Action Items for the Public Sector

Currently, the public sector offers three degrees of privacy protection, varying by nation or region:[10]

- Weak, ineffectual legislation in many parts of the world
- Comprehensive but scattershot legislation in the US, where up to 20 different regulations apply to privacy, and the only real focal point for privacy is the FTC
- The strictest legislation in the EU, in the form of the GDPR

While we believe the GDPR may go too far, we also believe other governments should get their privacy acts together. To that end, the US should simplify and codify its laundry list of regulations into one unified, easy-to-navigate privacy policy. Other nations should craft meaningful privacy reforms incorporating the only sensible provisions of the GDPR: those concerning Consent, Right to Access, and Breach. Beyond those location-specific recommendations, our action items for the public sector are as follows:

The US should simplify and codify its laundry list of regulations into one unified, easy-to-navigate privacy policy. Other nations should craft meaningful privacy reforms incorporating the only sensible provisions of the GDPR: those concerning Consent, Right to Access, and Breach.

1. Give consumers the right to sue for privacy violations, regardless of industry or sector.

The idea that US patients can sue healthcare providers for medical malpractice but not for 'data malpractice' renders HIPAA far less effective than it could be. Sometimes the threat of a debilitating lawsuit is the right medicine to persuade any industry to do the right thing. The US Congress should do elective surgery to remove this provision and allow patients to sue for privacy violations by healthcare providers, as well as create a national data breach notification law similar to the Breach provision of the GDPR. US legislators and industry alike worked together to pass HIPAA in order to protect the privacy of patient health information (PHI). Now, the parties need to close the loop by allowing patients to sue providers who do not honor their commitments under HIPAA. More broadly, to the extent that any industry has special, protected legal status anywhere, laws should be amended to eliminate those protections.

[9] Alliance of Automobile Manufacturers, available here

[10] DLA Piper, *Data Protection Laws Of The World,* available here

2. *Specifically* regulate how companies can use consumer data.

Many regulations seek to define how companies can store and use consumer data—and the EU's GDPR restricts data usage more extensively than any such regulation to date. What we are calling for are more specific guidelines, including which types of data companies can store; that the data be encrypted and otherwise protected to guard against compromise; precisely how long companies can retain data; what the data can be used for; and who owns the data. On the last point, we assert that the principle is simple: if you (person or entity) create the data, it is your data to do with as you wish, without limit and without impedance.

3. Aggressively use regulations already on the books to punish privacy violators.

Especially in the US, there is a perpetual thirst among many to fix any problem by "passing a law," without learning whether applicable laws exist. In many cases the key is not new legislation, but enforcing existing legislation. Figure 2 illustrates the point, presenting key US privacy regulations.

Figure 2: Overview of Key US Privacy Regulations

Regulation	Description
Federal Trade Commission (FTC) Act	Prohibits unfair or deceptive practices, and covers privacy and data security issues in online and offline (real-world) venues.
Federal Wiretap Act	Makes it illegal to intentionally or purposefully intercept, disclose, or use the contents of any wire, oral, or electronic communication through the use of a device.
Electronic Communications Privacy Act and Computer Fraud and Abuse Act	Regulate intercepting electronic communications and computer data.
Children's Online Privacy Protection Act (COPPA, enforced by the FTC)	Includes a wide range of measures designed to specifically protect the privacy of children, including an expanded definition of personal data to include geo-location data (location analytics) and cookies.
Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)	Regulates collection and use of email addresses.
Telephone Consumer Protection Act	Regulates collection and use of phone numbers.
California Invasion of Privacy Act (CIPA)	Makes it illegal to wiretap, eavesdrop (monitor) and record telephonic communications, and record mobile communications, without consent.
USA Freedom Act	Ends (theoretically, at least) the National Security Administration's bulk collection of data records—e.g., "Mobile Carrier X, we need records of all traffic between LA and San Francisco from last week"—that was the most concerning aspect of the NSA's data activities.
Health Insurance Portability and Accountability Act (HIPAA) and HIPAA Omnibus Rule	Regulate the use and sharing of protected health information (PHI).
Financial Services Modernization Act (Gramm-Leach-Bliley Act)	Regulates collection, use, and disclosure of financial information; limits disclosure of personal data; requires financial institutions to provide notice of privacy practices, and enables individuals to opt out of having their data shared. However, no single law governs when financial institutions must notify either customers or government regulators when a data breach has occurred.
Fair Credit Reporting Act and Fair and Accurate Credit Transactions Act (FCRA/FACTA)	Regulate use of personal data by consumer reporting agencies.

Sources: Federal Trade Commission, Thomson Reuters, Epic.org, Lawyers.com, Ellis Law Group, LLP, and Stratecast

Action Items for the Citizens/Consumers/Users

Our action items for citizens/consumers/users are as follows:

1. Secure your networks!

Consumers should always secure their networks. On routers and any IoT-connected device, this means changing the username and password from the factory defaults. They should also view their home network the way hackers do, and act accordingly. Users can visit a site published by solutions provider Bullguard[11] to discover whether devices in their network are visible on the Internet—and if they are, contact their ISP and device manufacturers. Other actions users can take include:

- Purchase a new router built specifically to address IoT privacy. Several manufacturers have introduced routers designed to do so.
- Update all devices. Today, this means not only computers but smartphones and all wireless devices, TVs, connected home devices, and more.
- Use a password app to create and keep track of a unique password for each service.

Also, device placement can be crucial. Users should not place any device that can stream video and audio to the Internet in any area of home or office they would prefer to keep private.

2. Before providing data, ask what it will be used for.

Commercial interests are accustomed to demanding all sorts of information from consumers; and consumers are accustomed to agreeably providing information. That needs to stop. Before providing their personal data, consumers need to ask how it is going to be used—and make sure providers are true to their word. Any interaction followed by a flood of new ads or messages on the topic should raise red flags.

3. Push for manufacturers to build privacy into products; lobby for stronger legislation.

Consumers should use the power of social networks to press manufacturers and all in the IoT ecosystem to build privacy into their devices and solutions. Citizens should also lobby their government representatives to enforce privacy legislation—and ensure that legislation protects their right to sue for privacy violations, regardless of industry or sector.

4. If your privacy is violated: take 'em to court.

If individual privacy violations occur, engage an attorney to file suit against the company or companies involved. While not all parties injured by privacy violations have the wherewithal (and knowledge) to file lawsuits—indeed, that is one of the main reasons for the existence of privacy regulations—individuals are, indeed, filing suit over privacy matters, as discussed in one of the three companion reports to this one.[12] If large-scale privacy violations occur, petition for a class-action filing, and communicate with groups such as the IoTPF and FPF.[13]

[11] The site is available here; more information about Bullguard is available here.

[12] The companion report cited is Stratecast, *We Have Seen the Future of IT, and it is Big Data: Part 1 – Will IoT Privacy Issues Steal the Future?* (BDA 5-01) June 2017; available here.

[13] IoTPF, available here, and FPF, available here

Stratecast
The Last Word

The future of IT is big data; and the biggest threat to big data is the issue of privacy. In the absence of meaningful progress on privacy in the private sector, governments are eager to jump in and make a difference—and some more than others. **The EU has jumped in with both feet in the form of its GDPR; but in so doing, it has a foot on the throat of business potential in the region.** This is a harbinger of things to come in other world regions if the private sector does not get privacy right in a hurry.

Stratecast is here to help. Our Privacy Blueprint, presented and analyzed in this report, offers specific recommendations for what the private and public sectors both need to do right now; as well as the group most affected by the actions those two groups take: the consumers/citizens/users whose data and privacy are at stake. The private sector needs to focus on standards, technologies, and establishing best practices. Those doing business in the EU and the UK need to put our GDPR Survival Plan into practice—and make at least some of what that entails standard practice for all data from all regions. The public sector needs to provide meaningful alternatives to the EU's draconian measures, and empower consumers to help in the privacy fight. For their part, consumers need to secure their networks; keep a close eye on what data they share with which parties; push for the private sector to make good on its privacy promises; and use the legal system to hit privacy violators where it hurts the most.

Thanks to the EU, the prospects for big data are not nearly as bright as they were before passage of the GDPR. This Privacy Blueprint and its GDPR Survival Plan, however, are designed to help all parties keep that once bright potential in focus.

Jeff Cotrupe

Industry Director – Big Data and Analytics

Stratecast | Frost & Sullivan

jeff.cotrupe@frost.com

About Stratecast

Stratecast collaborates with our clients to reach smart business decisions in the rapidly evolving and hyper-competitive Information and Communications Technology markets. Leveraging a mix of action-oriented subscription research and customized consulting engagements, Stratecast delivers knowledge and perspective that is only attainable through years of real-world experience in an industry where customers are collaborators; today's partners are tomorrow's competitors; and agility and innovation are essential elements for success. Contact your Stratecast Account Executive to engage our experience to assist you in attaining your growth objectives.

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies? For more information about Frost & Sullivan's Growth Partnership Services, visit http://www.frost.com.

CONTACT US

For more information, visit www.stratecast.com, dial 877-463-7678, or email inquiries@stratecast.com.