Kelley Vick:

Welcome, everyone, and thanks for joining us on today's panel discussion webinar, Critical Steps to Manage CCPA Compliance and Risk in 2020, brought to you by the IT GRC Forum.

Kelley Vick:

The IT GRC Forum produces educational events for the governance, risk management, and compliance community and we provide free market intelligence to all of our members. If you're not already a member, you can register at executiveitforums.org.

Kelley Vick:

I'm Kelley Vick, the host of today's program, and it's my pleasure to introduce today's speakers. Today's moderator is Colin Whittaker, welcome back to Colin.

Kelley Vick:

Colin is the Founder and Director of Informed Risk Decisions and has over 30 years experience in cybersecurity in government and in the private sector. Since retiring from the military in 2001, Colin took up the role of Head of Security at APACS.

Kelley Vick:

In 2010, he became the VP of Payment System Risk at Visa Europe where he sat and managed the risk appetite for all those processing, accepting card payments throughout Europe.

Kelley Vick:

Colin went independent in 2015 in order to provide businesses large and small across all sectors the benefit of his experience. He currently provides cybersecurity risk consultancy services to a wide range of public and private companies.

Kelley Vick:

Colin's goal is to help enterprises make reasoned, informed decisions about they protect and secure their critical information assets from cyber attack and meet regulatory expectations.

Kelley Vick:

He's presented on information security at major events around the world and has published a number of papers on security.

Kelley Vick:

And on the panel, we have K. Royal, Associate General Counsel at TrustArc. Ilia Sotnikov, Vice President of Product Management at Netwrix. Dr. Else van der Berg, Head of Policy and Product Strategy at Datawallet. And Harold Byun, Vice President of Products at Baffle.

Kelley Vick:

We'll run through a more detailed introduction with our panel in a moment. But first, I'll go over the housekeeping, learning objectives, and the agenda for today's session.

Kelley Vick:

First, the webcast is streaming live and all lines will be in listen only mode for the duration of the conference. If you have any issue with the audio, please first check your device settings before contacting technical support.

Kelley Vick:

And we recommend that you paste our direct landing page into a fresh browser window and close any other live windows to avoid conflicts. The direct console URLs are displayed on your screen now and they're clickable in the attached PDF slide deck.

Kelley Vick:

After today's session, we'll be providing one NASBA approved CPE credit to qualified attendees. To qualify and receive a certificate of completion for this program, we require that you've completed all fields on registration, answer all the polls, and rate us at the end.

Kelley Vick:

You can participate in the polls by submitting your responses in the box below your console. Just make sure the console is not in full screen mode or you will not see all the options.

Kelley Vick:

Please leave us your rating and feedback through the ratings tab. Or alternatively, you can use the evaluation form attached. We value your input and suggestions.

Kelley Vick:

And for those who qualify for CPE credits, certificates will be issued via email within 30 days.

Kelley Vick:

We're also taking your questions throughout today's discussion. You can submit these at any time using the question button. And if we don't manage to answer all of the questions that come in today, we'll respond by email.

Kelley Vick:

If you'd like a copy of the slides, you can download these through the attachments tab where you can also access the related white papers and resources at any time during the discussion.

Kelley Vick:

And finally, after the live presentation, this webcast will be available on demand. So please share with any colleagues you think may be interested in the topic. And watch your email for announcements about other upcoming webcasts which you can also find listed on executiveitforums.org.

Kelley Vick:

Our learning objectives today are to gain insight on understanding the nuances, ambiguities and challenges of the CCPA. Creating compliance programs in the midst of the unknowns. Developing a strategic action plan to become CCPA compliant. How to avoid expensive fines, class-action lawsuits, and injunctions. And getting ahead of the curve and enabling your business with alternate data sharing and privacy preserving techniques.

Kelley Vick:

Moving on to the agenda, I will begin with speaker introductions before running over some quick tips recommended by our panel. And then we'll dive into the Q & A discussion facilitated by Colin, before closing with takeaways and further information at the end.

Kelley Vick:

So now without further ado, I will go ahead and turn the program over for today's discussion. So over to you, Colin?

Colin Whittaker:

Thank you very much [inaudible 00:04:00] Kelley and good afternoon, everyone. To start with, I'm going to roam around the table and hear from each of our panelists. I'm going to invite them to tell us a little bit about their organizations and a little bit more about themselves so everyone listening today, either live or if you're listening later on the archive, can understand our panelists frame of reference for today's discussion.

Colin Whittaker:

Unfortunately, I'll let you know now that Else hasn't been able to join us yet. And hopefully, she'll be able to join us later on as the session continues. But to kick off with discussion, I'm going to start out with Ilia. So Ilia, if you'd tell us a little bit about yourself please.

Ilia Sotnikov:

Sure, thank you and thank you for having me here. So my name is Ilia Sotnikov. I am Vice President of Product Management for Netwrix Corporation. We are a software company helping customers all over the world with automating their compliance controls and security controls specifically around data security.

Ilia Sotnikov:

Understanding what is going on in the IT infrastructure, who has access to what kinds of data. What data do you have in the IT infrastructure, in the file shares, SharePoints or [inaudible 00:05:14] data or in the databases that support applications.

Ilia Sotnikov:

We also span into the cloud environment. And my role in product management is to work with the partners and with the customers to help them apply the best practices and to understand what are their needs and how we can help them achieve those goals.

Colin Whittaker:

Thank you very much indeed, Ilia. And thank you, I'd like to move on to K. Can you tell us a little bit about yourself and the work you're doing there at TrustArc?

K. Royal:

Absolutely. Thank you so much. So I am the Associate General Counsel at TrustArc. Prior to this role, I actually ran a lot of the consulting engagements that we have. So I've worked with companies from large to small, from tech and non tech all across the world to develop their privacy programs.

K. Royal:

And that's actually what TrustArc does. We are the world's largest and oldest privacy company. We've been doing this since 1997. We're a technology company that funny enough, we just acquired Nymity. And Nymity, a lot of people may also be familiar with. One of my absolute favorite resources.

K. Royal:

And so with that, we bring the power of privacy to everyone. And we have a consulting division. And so if you need help, just guidance, where to get started, not sure where to go now, we can solve all the needs on privacy whether it's consulting or technology.

Colin Whittaker:

Thank you very much indeed, K. And thank you, Else for joining us. I just warned everyone that you might not be with us and you joined us really rapidly just before your slide come up. So over to you. Can you please share where you're coming from today in today's discussion, please?

Dr. Else van der Berg:

Yes, definitely. Firstly, very happy that I managed to dial in. [inaudible 00:06:59] had some trouble. Yes, so my name is Else. I am the Head of the Policy and Product Strategy here at Data Wallet, which means that I am responsible for monitoring all the privacy laws in US and also monitoring [inaudible 00:07:16] to make sure that our product is compliant at all times.

Dr. Else van der Berg:

I hold a PhD in Law. And before this, I've worked as the Head of Products before a multiple Fintechs, which means that I'm quite comfortable on this whole intersection of law and technology and find it a fun field to work in.

Dr. Else van der Berg:

A bit of explanation about Datawallet. Datawallet offers a tool called Datawallet Consumer First Compliance which sounds like your basic compliance tool, but goes a bit beyond that.

Dr. Else van der Berg:

Firstly, of course we make sure that your business is compliant with the CCPA if you use our tool. We mainly focus on handling data subject requests, but can also go beyond that.

Dr. Else van der Berg:

But what makes us really special is the fact that we focus very much on the customer journey. We really aim to put consumers first and make sure that they have the controls and the transparency that they need in order to feel like they have a trusted relationship with the companies that they work with.

Dr. Else van der Berg:

We truly believe that that is where this whole ecosystem has to move to because consumers will no longer with businesses if they have no trust. So that's the most important stuff about me and about Datawallet.

Colin Whittaker:

Thank you very much indeed, Else. Last but definitely not least, Harold, can you give us an insight as to what you're doing at Baffle, please?

Harold Byun:

Sure. So my name's Harold Byun. I head up product management at Baffle. And so I've been working in the security space for over 25 years. I started on the security architecture and E-Commerce side of things.

Harold Byun:

A lot of my career has been focused on what I would call data containment so I worked with a data loss prevention solution which was a leader in the market back in the early 2000s or mid-2000s. And evolved into mobile security, different types of containment strategies. And more recently worked at a cloud access security broker.

Harold Byun:

Baffle really offers a simplified, data centric protection solution. And what that means in the context of data privacy regulations really enabling protections of the actual consumer data and PII values.

Harold Byun:

Most companies have been opting for years to implement what we would call a check box security approach to this problem. And the lack of actual data protection is evidenced by the latest breaches that probably happened yesterday, today or whatever is going to happen tomorrow.

Harold Byun:

And typically enabling this type of protection model has been very, very intrusive and requires modification of applications and it's difficult to achieve. And what Baffle does is ultimately provide this protection via a No Code model to simplify and ensure compliance with data privacy regulations.

Harold Byun:

So there's a whole suite of capabilities that we have, including dynamic data masking and record level encryption. Bring your own key services that are offered in a simplified manner.

Colin Whittaker:

Brilliant. Thank you very much indeed, Harold. I think we're very privileged everyone to have two lawyers on the panel as well as two technicians to talk us through this very complicated issue of how these regulations will apply and play out.

Colin Whittaker:

So I think they've all set the stage. Our panelists [inaudible 00:10:24] those really well for this afternoon's discussion.

Colin Whittaker:

So to kick things off, we've had each of our panelists identify some quick executive tips for you out there in the audience which they'd like to recommend and highlight before we get into the detailed discussion and questions.

Colin Whittaker:

Some of the things we're talking about here about the CCPA applies to everyone. But it's just not a beginning of regulations. There'll be more to come.

Colin Whittaker:

It's clearly going to cost a lot more money than the estimated costs projected by the Attorney General. These things always do. I think we can all appreciate that.

Colin Whittaker:

Don't wait to comply. Compliance it's not standalone. It's the extension of the customer journey. A bit what Else will be talking a little bit more about, I'm sure. And it should be no more then the bare minimum we're doing.

Colin Whittaker:

Also, that privacy regulations are not going away. I think everyone that's been watching this landscape for the last few years can say that. We should be starting to look at alternative data sharing and privacy preserving techniques to get ahead of curve, enable our business to operate in this privacy rich environment.

Colin Whittaker:

So I'm going to invite our panelists to tell us a little bit more about this. So Ilia, we're going to start with yourself. So what's your quick tip for our listeners regarding the new CCPA regulation?

Ilia Sotnikov:

Thank you, Colin. So yeah, like you said, it's great to have both the legal and the technical aspects represented on this panel. So I hope that our colleagues here will correct me if I'm misrepresenting anything. I'm coming from the technical side of this.

Ilia Sotnikov:

And working in a software company, we are talking to a lot of folks in the IT operations, the management level, directors, VPs of IT operations. We are also talking a lot to the IT security side of the house. And like I said globally, with almost 10,000 globally.

Ilia Sotnikov:

And a lot of people are asking this question and a lot of people are seeking this kind of guidance, should we be worried about CCPA? Should we be worried about GDPR if we are located in this or that state or here or there? If we are doing business internationally, what should be on the top of our list and what should we be thinking about?

Ilia Sotnikov:

And the real answer is that in the modern economy, regardless of where you are, if you are doing business online, if you are in any of the states and doing business nationwide, absolutely you are going to have customers from California. That's unavoidable.

Ilia Sotnikov:

And if you look at the criteria of CCPA, you definitely can see one of those three criteria. Upwards in 25 million in annual revenues or you have more than 50,000 records collected on an annual basis. Or you're deriving more than half of your revenues from selling the personal information.

Ilia Sotnikov:

So if either of those three applies to you then you absolutely have to apply CCPA and you have to comply with this.

Ilia Sotnikov:

And like the slide says here, it is just a beginning. You see that similar regulations are popping up all over the globe actually. Not just within the United States. It is very likely that there will be the federal regulations coming up. Probably not immediately, but eventually.

Ilia Sotnikov:

So you definitely should work on understanding what exactly applies to you, but definitely, definitely be prepared. This is not going away any time soon.

Colin Whittaker:

Thank you, Ian. That's a really good start. Thank you for that indeed. K, can I turn to you now and ask what your starting tip is and can you tell us about your perspective of the costs associated with noncompliance?

K. Royal:

Oh, absolutely happy to help here. And this is one of the questions that I get from every company we work with is exactly how much is this going to cost?

K. Royal:

And not just terms of money, but also in terms of effort and other resources. And one of the biggest things that I can recommend is that companies understand that you may not have previously associated a budget, much less a large budget, to data protection or privacy efforts.

K. Royal:

Maybe you have the security, but not in the angles that the CCPA and other privacy regulations are looking at.

K. Royal:

So just understand that this isn't going to be cheap. I mean I'm sorry, if that's the route you want to take and order, then you're probably not going to be able to handle your data properly. And you probably will run afoul of the CCPA.

K. Royal:

And given that the CCPA is the first one to allow a private right of action for data breaches and, potentially, for other privacy violations. There's some muttering going on around that, then you need to understand, there is a huge cost associated with this.

K. Royal:

There's technology and vendors out there absolutely available to help you. We're four of the ones on the phone here.

K. Royal:

But as a personal note, I want to add that did anyone read the cost projections from the Attorney General's office when they passed the regulations? It is a fascinating read.

K. Royal:

But one of the things in there and here's where the cost projections come out. The cost projections are that the CCPA is only going to cost small businesses $25,000 for the first year and an ongoing of $1500 a year.

K. Royal:

$1500 to manage privacy in your company. Now they'll say, "Oh, well we're not a small business." Because the typical business is only estimated to spend $2500. And in the justifications for this, they actually said that training is free because it would be logical for companies to have their privacy people already know about CCPA so there shouldn't be any cost to training.

K. Royal:

So please just understand that this is a significant regulation. You need to take a deliberated and conscious approach to it. And make sure you look at it as a very serious compliance obligation and tackle it in the right way.

Colin Whittaker:

K, thanks very much indeed. I mean I can reiterate the cost implications from advising some clients on GDPR implications in Europe. And I would agree that whatever you think the budget is perhaps at least double it and think again. Because it's going to be [inaudible 00:17:16] burden going forward.

K. Royal:

Exactly.

Colin Whittaker:

[inaudible 00:17:20]. Else, can I turn to you now? What sort of recommendations would you make and tips would you provide to set the stage for today's conversation?

Dr. Else van der Berg:

Yeah, sure. Thank you. So number one, I think everybody's who's listening to this already actually knows. It's the fact that becoming compliant with CCPA is very, very complex. And it touches basically all of the verticals of your businesses. And also requires them to collaborate with each other.

Dr. Else van der Berg:

I'll just dive a little bit deeper into one aspect of the CCPA to give you a clear understanding of how big the scope actually is. And I'd like to talk a little bit about the data subject requests.

Dr. Else van der Berg:

So to comply with this requirement of the CCPA, firstly, you would need to make multiple contact methods available, which could be a phone number, email address, or a web form.

Dr. Else van der Berg:

And then when you've done that, you need to be able to actually handle these requests. Which starts with verifying the identity of the consumer, [inaudible 00:18:12] for exceptions in the law, and then actually finding all the data across your systems. Either deleting it or aggregating it or de-identifying it.

Dr. Else van der Berg:

Or in cases of [inaudible 00:18:23] no gathering of the data and then making it available in a way that follows this requirement of reasonable security measures.

Dr. Else van der Berg:

So that's just one small aspect of CCPA. And you can already see that it touches a lot of different things. Firstly, you would need to change your website. You'd need to get your operational processes up and running to be able to handle these incoming requests.

Dr. Else van der Berg:

You need to establish all kinds of processes to be able to check for these exceptions. You need to maybe change your IT infrastructure. And it goes on and on and on. So that's just one aspect of CCPA.

Dr. Else van der Berg:

So what I'm trying to say is to try to become fully CCPA compliant without any outside help will be extremely complicated. And it's also still very [inaudible 00:19:04] and expensive. So I would like to recommend strongly against that.

Dr. Else van der Berg:

And then to continue with the other bullet points, what is quite important with these data subject requests that I just touched upon is that they go beyond just compliance.

Dr. Else van der Berg:

A lot of businesses we talk to want to just be compliant and be done with the whole thing. But actually these DSRs, data subject requests, they extend the customer journey.

Dr. Else van der Berg:

And you may have gotten your customers through a marketing campaign or a sales call which was your first touch point with the customer. And this whole life cycle continues through there.

Dr. Else van der Berg:

And actually the handling of these requests, it's just another touch point with your customer where you can either disappoint them or make them really happy.

Dr. Else van der Berg:

It's the same as customer support. So either you lose your customer or you keep him. But we notice very often with businesses that this side is neglected which is actually really a shame. Because if you make sure that your customers are happy and feel that the interface that they're using is beautiful, uncluttered. They understand what they're doing. You can actually save a lot of data points that you stand to lose under the CCPA.

Colin Whittaker:

Else, brilliant. I think it really sets up the discussion nicely there for later on. That's wonderful. So Harold, finally over to you. What other recommendations would you like to highlight before we move into the Q & A?

Harold Byun:

Yeah, again, I think re-emphasizing what other folks have already said is that privacy regulations are not going to be going away any time soon. So you should really start looking at alternate sharing and privacy preserving techniques to get ahead of the curve and see what you can do to enable your business.

Harold Byun:

Ultimately a lot of the folks focused on data privacy compliance are ultimately looking at ways to stop collecting data. And I think that the reality of most businesses is that people aren't going to stop

collecting data. And obviously it gives the consumer a certain amount of controls, specifically the right to be forgotten or the right to be deleted.

Harold Byun:

The right to not have their data re-sold and ultimately the right to control how their data is being used. I think that the challenges for the business is ultimately looking at it from a competitive landscape.

Harold Byun:

And with the, obviously, extreme focus on machine learning and artificial intelligence, there are ways that obviously people are looking to intuit and infer things about the consumer and their preferences in order to ultimately, in the best world, deliver a better service or a better product offering or a better set of capabilities for that consumer.

Harold Byun:

And I don't think that that need is going to go away. And so within that context, there are capabilities that are available. There are technologies that are available in market that allow you to anonymize the data and still run aggregate analytics on the data in what we would call a privacy preserving technique.

Harold Byun:

In utilizing these methods, you can still comply or not violate the data privacy contract or the confidentiality contract that you have over the data set that you hold and still derive business intelligence and analytics from that data.

Harold Byun:

And so this slide is really meant to show on the top half, the consumer desires or the consumer rights within CCPA. And potentially some mitigation strategies or data management strategies that an organization who holds that data could take.

Harold Byun:

So the ability to shred data and the ability to revoke it or, in theory, mask and delete it on the fly, as well as just privacy preserving analytics capability.

Harold Byun:

And then one other added note around this data sharing aspect of things is that one of the Opus Ponemon surveys that was released in 2018 surveyed a 1000 CSOs and posted two thirds of them had had a breach via a third party.

Harold Byun:

And so there's this whole notion of managing third party risk and data sharing strategies across third parties because under the CCPA regulation, you are actually responsible for your third party relationships and how they handle data.

Harold Byun:

And if they have a breach, then you are responsible for that by virtue of having that relationship. And roughly, again, two thirds of those CSOs claim that they had a data leakage or data breach incident via a third party in that survey.

Harold Byun:

So something else to consider in terms of how you want to shore up your data protection strategy going forward.

Colin Whittaker:

Harold that's brilliant. Thank you very much. I'm sure we'll dive into all of that a lot deeper as we go on during the Q & A.

Colin Whittaker:

So I think that sets [inaudible 00:23:43] really nicely the discussion. I think you heard where our panelists are coming from, where they [inaudible 00:23:47] fit, and where they represent their companies and where their interests lie. So this is really brilliant stuff.

Colin Whittaker:

So we're going to pause there for a moment on the slide with everyone's head shot, have titles and affiliations so that everyone listening today can put a face to the voices that they're listening to.

Colin Whittaker:

And everyone out there in the audience, I do want to remind you that it's very much an interactive session. And we have some great talent assembled, as you already heard. So please don't be shy and use the question tab liberally. And I'll be monitoring that for your input. And I'll try and weave your questions into the questions that we've already got established.

Colin Whittaker:

And fortunately, we've already got three people that's asking questions. And I'll try and weave those in as soon as I can in the discussion.

Colin Whittaker:

So to kick off, I think it's important to reflect on first of all, why we've got these privacy regulations in the first place. And particularly to scope out the impact of the CCPA.

Colin Whittaker:

And I think it's important to remind ourselves that this isn't the only data privacy legislation we have around that we're all worried about. Or indeed that will maybe come along in the near future to bite us all and what we're doing.

Colin Whittaker:

Therefore, I'd like to start with asking a question of Ilia. CCPA provisions and privacy regulations, Ilia. Other states are adopting similar ones to what GDPR represents both in the US and beyond that. So why do you think that other countries and states are, indeed, following the example of GDPR?

Ilia Sotnikov:

That's a great question. Thank you, Colin. Even in your example, GDPR is not necessarily the first regulation in the realms of privacy. And actually countries in Europe, European Union, went forward introducing GDPR on top of the various local regulations that they had in place already. And they were, I believe, like something like 28 country members.

Ilia Sotnikov:

So GDPR was on one hand just an attempt to normalize those regulations to allow businesses work in the same environment across all of those state members of the European Union.

Ilia Sotnikov:

But on the other hand, what GDPR really marked was a break in this situation where consumers and citizens did not really realize how much data is being accumulated by the various businesses, especially in the online environment with those internet giants.

Ilia Sotnikov:

And one of the big statements that GDPR sent to the global public was that it is really important to be the owner of your privacy. It is a big concern and raising concern across various nations.

Ilia Sotnikov:

And I think that GDPR specifically introduced those pretty hefty fines for noncompliance and for abuse of those rights in regards to how do you treat the consumer information that you collect.

Ilia Sotnikov:

So that sent a message and I think that was one of the biggest reasons why in various other jurisdictions, like in the United States or in Australia or in Brazil. A lot of other countries and a lot of others legislators started to look into how can we protect our citizens? How can we protect their private data?

Ilia Sotnikov:

And CCPA and GDPR are not an exact match. GDPR goes into lengths on how exactly you should map, for example, your data flows or things like that that CCPA does not require.

Ilia Sotnikov:

But I think the important note here is that GDPR really marks that urgency and that public interest for protection of this kind of data that was not necessarily recognized before. And that's why there is so much followers and so many examples of other countries introducing that kind of regulation as well.

Colin Whittaker:

That's very useful. Thank you, Ilia. I think one of the concerns about all this data privacy laws is trying to understand what is they're trying to protect? And perhaps we ought to reflect on what data is actually personal information and what people consider to be personal information. Wherefore the regulatory risks might lie if there was a data breach or a privacy breach.

Colin Whittaker:

So we've actually been running a poll which has been running for some time. And for those who aren't used to the poll, the polls can be underneath and we've already had 199 people responding. And we're asking the question about what personal information do you think is the highest risk under the new CCPA regulations?

Colin Whittaker:

Is it social security numbers, passport numbers, biological information and so on? For those who haven't responded, I encourage you to respond as soon as you can. And the options, they're below your console. Just make sure you're not in full screen mode or you won't be able to see these.

Colin Whittaker:

And remember that participation is required for your CPE credit. The poll will remain active for another few minutes while we consider the responses.

Colin Whittaker:

And while you're doing that and for those who haven't responded [inaudible 00:29:44] or yet, I'll turn to K. K, we were just talking about GDPR there with Ilia.

Colin Whittaker:

And GDPR came to us, I think, and I'm saying that from a UK perspective and a European perspective, I think it was really the first significant, new privacy law.

Colin Whittaker:

And many enterprises, particularly in the US, I know spent a lot of time implementing those, the GDPR regulations, to be compliant with them. So what more do you think these enterprises have to do if they're going to be ready for CCPA? Is it something new? Is it something different? Or is it broadly the same sort of thing?

K. Royal:

Well, actually it's the baseline is the same thing. What you're looking at is controlling data and then putting control of the data in the hands of the individual whose data it is and being transparent about it.

K. Royal:

But there are some very key differences between the CCPA and the GDPR. Differences that companies who are already GDPR compliant need to pay attention to.

K. Royal:

One of them is, and I think we're going to get to vendors here in a little bit, but one of the biggest things is the vendors. There is a difference between processors under the GDPR who are directly liable to the supervising agencies for their practices and then service providers under the CCPA which are not directly liable to the regulators.

K. Royal:

So that is a key difference. You need to understand as a business that you need to have the right protections and agreements in place with your service providers. And also that there is a big difference in service providers versus other third parties that you might be providing data to.

K. Royal:

So make sure that you identify where your data goes and what issues you have with it.

K. Royal:

Now there are some key differences in the individual rights management. The CCPA has some exceptions that are not provided under the GDPR for the right to deletion. Also for access, it's limited to the past 12 months.

K. Royal:

But I think one of the biggest differences is what you need to put in your publicly available privacy notice. Now you have to have a privacy notice whether it's online or offline activities.

K. Royal:

But in most cases, it's going to be an online privacy notice. And the biggest difference is you have to be able to identify where you are selling data. Now you can't see me, but I'm doing air quotes around "selling", because it has a unique definition under CCPA. Here's my air quotes.

K. Royal:

It's exchanging data for anything of value. And so you need to get legal involved to see where you're sharing data, is that sharing it for something of value? Not necessarily money.

K. Royal:

One of the common examples given and I'm not saying this is a sale or not, but one to help you understand is are you getting free website analytics in exchange for them getting the data they can scrape off your website?

K. Royal:

So that might be something you need to consider. And the hardest parts of these are the fact that where a lot of data sharing happens that may be the privacy or the security person isn't aware of is free services or low cost services.

K. Royal:

You never know when a rogue employee is going to see something free and say, "Oh let me use this." And they're sharing personal data there. So you need to be able to identify where your data is going.

K. Royal:

If you do your data inventory and mapping and you identify that you are not "selling", again air quotes, "selling" data under the CCPA, you actually have to state in your privacy notice. You have to state, "We are not selling data."

K. Royal:

And you may be aware of this, here in the US, but if you state something in your privacy notice online that is true, you either say you do something that you don't or say you don't do something and you actually are doing it, you might fall under regulation from other agencies such as the Federal Trade Commission who tends to enforce public privacy notices as an unfair and deceptive trade practice.

K. Royal:

So if you're going to put that in your privacy notice, you need to make sure that you have reviewed all of your data practices and made sure you are not selling data for something of value.

K. Royal:

Those are the biggest differences, I see, between the CCPA and the GDPR. But there are key differences that you can't just assume that you're compliant with GDPR and, therefore, you're good with CCPA.

Colin Whittaker:

Thank you very much indeed for that, K. Before we move on, would you like to offer any observations from the response to the audience for the question. Most people think that the social security number is going to be the biggest concern of CCPA. Do you share that? Or do you think some of this other information that we've talked about here is going to be relevant?

K. Royal:

It's going to be interesting. The social security number, of course, is one of the most common that we consider sensitive data. And here in the US, we use social security number basically for everything.

K. Royal:

And by the way, if you're carrying your social security card around in your wallet or your pocketbook, stop that. You shouldn't carry your social security card around with you.

K. Royal:

Anyway, back to social security number. So yeah, I do think that's going to be an issue, but the regulations from the Attorney General are trying to negate that information.

K. Royal:

So social security numbers should not be something that you provide to a company in order to verify who you are. And it's not something the company will be allowed to provide back to you if you are requesting access to data.

K. Royal:

So some of these sensitive information, including passport number is included in there is going to be interesting.

K. Royal:

I think one of the biggest ones is going to be the online tracking. I have to say I agree with people on that one because it's so hard for companies to manage what third party trackers are on their websites. Maybe they can control their own, but third party is hard.

Colin Whittaker:

Yeah, I think that's the bigger issue and I'm sure we'll come to that as we're going through the discussion. In fact, I think there are many nuances or shades of interpretation in the CCPA that we're going on to in the discussion here. The privacy laws.

Colin Whittaker:

In that sense, perhaps I best turn to Else now. Else, which consumer rights are introduced in the CCPA and how should these be handled? And particularly, I'm thinking of the one that K mentioned. What's your perspective on the do not track and what the Attorney General is saying about that at the moment?

Dr. Else van der Berg:

Sure, yeah. Thanks for the question. I can start by quickly listing these consumer rights and then go deeper into your other questions. The consumer rights, I think most of the people already know are, firstly, your right to know the information. The right to be notified of important information about data collection at or before the point of data collection.

Dr. Else van der Berg:

A right to have personal information deleted. A right to opt out of the sale of data. As K discussed, this term is quite wide and quite broad. And a right not to be discriminated against when a consumer exercises any of these rights.

Dr. Else van der Berg:

So this is already a pretty long list and it would be impossible for me to really go through all of them at this point. So I would like to also focus on two main aspects.

Dr. Else van der Berg:

And one of them, perhaps [inaudible 00:36:59] what K just mentioned which is these exceptions. The first aspect I would like to look at is the verification of consumer requests.

Dr. Else van der Berg:

I think this is very important because on the one hand, of course the CCPA is very good for consumers and it offers a lot of protection. But on the other hand, it can also be seen as an open door for fraudsters because they can quite easily impersonate people and try to get access to their data.

Dr. Else van der Berg:

So that's why there's a huge focus also by the Attorney General in [inaudible 00:37:31] proposed regulation on the verification of these requests.

Dr. Else van der Berg:

The second thing is the exceptions. There are global exceptions. There are exceptions specifically for deletion requests. And there are exceptions for requests for information.

Dr. Else van der Berg:

And that's the stuff that we just mentioned. Certain pieces of information may never be provided. Like the social security numbers, also passport numbers, account numbers, health insurance numbers. All super sensitive stuff like that.

Dr. Else van der Berg:

What happens with this is that actually a very high burden is placed on the team that is handling these requests because if they make mistakes in these steps, that can be very costly and can really damage the reputation of the business.

Dr. Else van der Berg:

So this is a team that might already be handling a lot of customer service requests. They have a huge, huge, huge new responsibility. And so that's, again, why I would recommend using a tool that maybe takes these things away from the team. Or at least guides them through it step by step.

Dr. Else van der Berg:

I don't think I have time to go much more in depth about every single consumer request, but I think everybody will receive a bunch of documents after this webinar. And one of them will also be a CCPA preparation guide which we prepared which goes way more in depth into this stuff.

Colin Whittaker:

Thank you for that, Else. That's a very useful insight. And it's a good reminder for everyone to actually troll through the attachments and links and download everything that they need from that. Because I've already done it and there's some really useful stuff there.

Colin Whittaker:

Harold, can I turn to you now? One of the important considerations is how we delete data. And you mentioned that at length in your introduction. And I think you'd want to return to that theme. So how

do you think data deletions and the rights [inaudible 00:39:20] and data replications best be handled with the technology that we have available today?

Colin Whittaker:

And I think you also had some observations you wanted to make on the poll as well, didn't you? So which would you like to start with?

Harold Byun:

Yeah, no, I mean I think I'll try and tie to the two together.

Colin Whittaker:

Thank you.

Harold Byun:

Yeah, I think when you look at the right to be forgotten or this ability for the consumer to make a deletion request, it ultimately does put companies in the position where they need to establish a very common notion of what I would call a consumer data record.

Harold Byun:

And that is on a record by record basis, you have information about the consumers that are engaging in business with your organization and there needs to be an mechanism to revoke that data facilitated by the consumer demand to do that. And effectively, instrumenting some form of kill process and kill button on behalf of the consumer.

Harold Byun:

There's a number of ways that people can do that. One of the ways that we're seeing some of the even insurance carriers approach this is really looking at a state by state model where you have subdivisions of the consumers based on the state that they reside in.

Harold Byun:

And then assigning what they're calling more or less a record level keying model on a consumer by consumer basis. And so the idea being that every consumer record has its on key or data owner ID that is ultimately mapped to the ability to present that data as well as the ability to delete or kill that data.

Harold Byun:

And so there's a number of different mechanisms that can be deployed from a technology standpoint. Record level encryption, consumer focused keys and distribution models in terms of bring your own key.

Harold Byun:

But being able to facilitate that from an actual execution standpoint, I think is what a lot of organizations are going to struggle with.

Harold Byun:

And within the context of the pool, I think that one of the other potential interesting insights about these PII or consumer based records is I could make the demand to kill my SSN or my personal data within a given organization.

Harold Byun:

But the reality is that the SSN, my SSN is probably already out there. And if you're a US citizen, your SSN is probably already there because it's probably already been breached 20 times over, if not more.

Harold Byun:

One of the other interesting areas that I do think is potentially of interest is actually biometric information. I believe that there was actually a pretty broad scale UK breach of biometric data.

Harold Byun:

And the reason that I think that this I interesting is because even if you delete it, you can't change your biometric information. And so my voice as my password or my retina scan or my fingerprints, those are things that I cannot easily change.

Harold Byun:

And so once those are compromised, they're out there and they're used as an authentication basis for whatever system of record are utilizing those. So I do think that that's a slightly, just a little bit of a different insight in terms of what people are focused on in terms of sensitive information.

Colin Whittaker:

I think that's a very useful observation on the biometric data though. [inaudible 00:42:27] you're quite right say in the UK, from the privacy perspective more than a data breach perspective. But yes, I absolutely agree that's increasing concern. And I'm sure it will be for regulators elsewhere in the world in the future.

Colin Whittaker:

Ilia, can I turn to you now? When it comes to things like CCPA, one of the questions, who does it apply to? Well, it broadly applies, I think, to most people who do business in California. But one of the questions [inaudible 00:42:54] people always ask, you think relevant for business for business exchange. Or is it just the business for consumer regulation. What's your perspective on how this plays out?

Ilia Sotnikov:

Yep, thanks. This has been a very confusing question. Actually, we as a B to B company are looking into this ourselves. And to the best of my knowledge and I know that the final regulations are still not out there and the Attorney General is still finalizing the text of the regulations.

Ilia Sotnikov:

The understanding that we have is that the CCPA in its full is currently applied to the B to C environments. And the companies that are collecting data from the businesses are exempt from this for a limited time.

Ilia Sotnikov:

However, this is just temporary and so you should understand that whatever, even if you are in a B to B environment, you need to consult your legal counsel. Make sure you fully understand what kind of data you collect. Where it resides. What you do with this kind of data.

Ilia Sotnikov:

And then make sure what regulations you have to adhere to. But even if it is not necessarily applicable to you right way, and like I said, this is temporary and you will have to comply with this later probably down the road. So you should still understand the best practices. Understand what are the processes and stay open to the news in this area.

Colin Whittaker:

Thank you [inaudible 00:44:57], Ilia. I think the point about B to B then is important because I do think there are lots of information that businesses share between each other of their employees and their own customers which will bring them into scope of the regulations.

Colin Whittaker:

And I think it goes back to what both Else and K was saying about the importance of mapping the data flow there on how information is shared and who you share it with.

Colin Whittaker:

Okay. So what we're going to now do is hopefully turn to some more tangible recommendations for our audience about what they can do and help their businesses to prepare and become compliant with this new law.

Colin Whittaker:

So before we go to much further, though, I want to see what implementation concerns our audience might have. Because we can seep those into the discussion as we're going on. So we're going to have our next audience poll which is all about what do you believe is the most difficult thing about preparing the CCPA.

Colin Whittaker:

Now as before that panel will remain open for about a minute or so and I encourage many of you to respond as you can in the time available. And while she is doing that, I'll turn to Else. So Else, how can an organization prepare for CCPA now?

Colin Whittaker:

In particular, because people take the perspective that the final regulations are not really published yet, the definitive substance to them. So how can they keep up with an ever changing and, perhaps, not interpreted by the regulators' view of what the law actually means and how they're going to apply it?

Dr. Else van der Berg:

Yeah, that's a very good question. We also see that a lot of businesses are actually struggling with this. As you may know, there was a comment period where people or organizations could comment on the draft regulations that were published by the Attorney General in October.

Dr. Else van der Berg:

And comment period ended on December 6th which led to about 2000 pages worth of comments, plus the transcripts of five public hearings.

Dr. Else van der Berg:

And you can see when you scroll this that it's full and full of questions for clarifications and other open questions. So based on that, it's actually impossible to estimate when the final regulations will actually publish.

Dr. Else van der Berg:

And at the same time, it's clear that businesses will not be able to adjust to these final regulations by the deadline of the 1st of January. Because either they would be too late or they would definitely not have enough time to get ready.

Dr. Else van der Berg:

There was an amendment to the CCPA that passed in September which introduced an enforcement delay for the Attorney General which states that Attorney General will only proceed with action after July 1st.

Dr. Else van der Berg:

Which gave a lot of businesses the idea that they could relax a little bit because it meant that they could wait with compliance efforts until July 1st.

Dr. Else van der Berg:

But actually yesterday, the Attorney General made some very clear statements and said that this enforcement delay does not at all impact the January 1st compliance deadline.

Dr. Else van der Berg:

Also, the law text itself states very clearly that the CCPA goes into effect on January 1st.

Dr. Else van der Berg:

And even then, even after the final regulations are published, we know from our experience with GDPR that the actual meaning of the terms of the law becomes apparent in the jurisprudence. So when the cases are actually brought to the court after.

Dr. Else van der Berg:

So that just brings more and more confusion. Sorry for that. But what I'm just trying to express that trying to stay on top of all of that by yourself, and also whenever you see a change happening in the legal landscape, [inaudible 00:48:26], it's like a legal game of Whack-A-Mole. You can never win and you would end up spending a lot of money and most likely still miss something that's quite important.

Dr. Else van der Berg:

So that's all bad news. The good news is that there are tools that help you and that people [inaudible 00:48:43] from you.

Dr. Else van der Berg:

So for instance, at Datawallet, we work with a team of legal experts that are completely making sure that we are most up to date for all the privacy regulations. That our product is also compliant with all of these regulations.

Dr. Else van der Berg:

So that's basically the best advice that I can give you is, again, try to not do it by yourself because it's virtually impossible. And look at a professional tool.

Colin Whittaker:

Thank you very much indeed for that, Else. And Else while you've been talking, some of the responses have come through. Do you share these priorities of concerns that people have raised? Like 68% of people are most concerned the most difficult thing will be detecting [inaudible 00:49:22] data. Do you share that from your experience?

Dr. Else van der Berg:

Yes, firstly on the votes from audience, I still see the old question. But I totally agree that the detection of data is a very complicated topic. A lot of large organizations, especially these organizations that will be in scope of CCPA, they do work with an acute data landscape.

Dr. Else van der Berg:

So detection is a very important problem that needs to be faced. Needs to be tackled. And is also something that we can help you with.

Colin Whittaker:

Thank you very much indeed for that Else. K, can I turn to you? You might have some observations about the responses as well. But as Else said, we really can't wait for legal interpretations and take the

learnings from case history, et cetera. So what are the top three things every company needs to do for CCPA?

Colin Whittaker:

Clearly privacy notices are one of those. And you might have noticed from some of the questions, people have some concern about privacy notice being just flannel in the life of the problem that they're going to have in the future.

Colin Whittaker:

So what's the three things you would probably recommend people do if they were going to do anything at all?

K. Royal:

Well, I will say and I agree with the feedback from the audience that it's going to be the discovering the data and where the data is going that's going to be the challenge.

K. Royal:

And so the three things that I have are not just my opinion, they're from the hundreds of clients that we've worked with. And the gaps that they have and the work that they need to put in.

K. Royal:

And my three recommendations fall right along that line. Data inventory is the first thing that any company can do. How can you possibly identify anything else you need to do with data? Such as disclose it in your privacy notice. Identify third parties. Identify where a sale might be happening unless you know what data you have and where it's going.

K. Royal:

My second one is data governance. I would put that in right along with your data. You need to make sure you stop with the data practices that clearly all the regulations are going towards. We can no longer collect as much data as we want, when we want and hold on to it for as long as we want.

K. Royal:

We need to collect data because it has a specific purpose and only use it for those purposes. Now does that mean you can no longer collect data that you want? No.

K. Royal:

What it means I identify a reason why you're collecting the data and then you have to be transparent about it. But that also means that your employees need to know that.

K. Royal:

So as part of your data governance, you need to make sure your employees are aware of this.

K. Royal:

And then privacy by design. I know we keep hearing that phrase over and over, but it really does mean that you need to involve your privacy professionals into your data governance practice. They need to own that and they need to be able to push it out.

K. Royal:

And so the three things were the data inventory, the data governance. And then the last one is the individual rights management. Again, clearly by the laws and the regulations, it is intended to put data management in the hands of the consumers or the individuals whose data it is.

K. Royal:

And so you need to make sure that you're able to accommodate individual requests. And I give these three things, looking at the GDPR, looking at HIPAA, looking at the CCPA, looking at the LGBD in Brazil, it's very common across all laws. And the laws that are expected to pass in the US, I imagine that these three things and including vendor oversight which I think Harold or Ilia may touch on.

K. Royal:

But they should be the commonalities across all the laws that you need to pay attention to those elements.

Colin Whittaker:

K, that's brilliant. You stole my thunder. I was going to mention data privacy so you actually got that one. The one thing I'd say, from my experience of dealing with people who've been going through the GDPR journey is really to well you're doing the data mapping is really, if you're supporting the business, start asking some difficult questions.

Colin Whittaker:

Asking difficult questions about why they've captured certain data and why they might not be using it. And clearly, the worst possible offenders in any enterprise that's doing that are the marketeers.

Colin Whittaker:

They've always collected so much information in the past. But half the information, they wouldn't even know to use that they've captured already.

Colin Whittaker:

So I think this is going to really ask some serious questions about how marketing and business development professionals use this data or what data they need to be able to do their job reasonably in the future. And [inaudible 00:53:54] going to help people resolve some of these dilemmas in the organization.

K. Royal:

Oh absolutely. And they need to question it. There was a company that I worked with that collected gender solely so they could identify the recipients of their marketing emails as Mr. or Ms. But they could only sell to doctors. So every single email was Dr. Gender was immaterial.

Colin Whittaker:

Yeah. And asking that question [inaudible 00:54:27]. Harold, I'd like to turn to you now. K mentioned right at the beginning about the fact that one of the differences between GDPR and CCPA is the obligations on third party.

Colin Whittaker:

But I know third parties are a major concern. So how do you think enterprises are going to operate with third parties in the future? And do you think this is a concern that many of your organizations that you're dealing with are sharing at the moment? And what recommendations would you be giving them under CCPA in respect to third party?

Harold Byun:

Yeah, I mean that's a great question. There are a lot of similarities between GDPR and CCPA related to third parties and overall responsibility. Obviously GDPR is making reference to specifically third parties that are performing data processing or handling data on your behalf.

Harold Byun:

And under CCPA, it's similar. Your company is responsible for any third party that house your data or your customer's data. And so obviously this is, as you all have been alluding to, vendors doing market analysis or re-marketing.

Harold Byun:

Any type of billing services. Even any type of health benefits for your employees. But customer service and support are obviously the third parties that are commonly reference vendors.

Harold Byun:

It's going to add a lot more burden on a couple fronts. I mean and related to the response from the viewers here about detecting and mapping data. If you think it's hard within your organization, once it leaves your organization's boundaries, it gets infinitely harder.

Harold Byun:

I mean everybody, I think, is familiar with these litany of questionnaires that you send to these third parties to more or less bless them as an authorized third party vendor.

Harold Byun:

But the reality is once the data goes over the fence, it's the wild wild West. And I think that that's going to put a lot more burden on organizations to really understand and, again, map the data that is going across to third parties. That's going to be part of the third party review and risk assessment.

Harold Byun:

And it's also going to require contract revisions in terms of the specifications and the mandates around data handling. So I think that those are all going to be additional challenges and additional overhead on the privacy and risk groups for a lot of organizations.

Harold Byun:

It's something that you're going to want to gear up for. An alternate model, again, that we may see continue to emerge is this notion of being able to consolidate what I would call the information supply chain.

Harold Byun:

And so a lot of these third parties have a portion of your organization's data or your customer's data because you've basically taken this information supply chain and everybody that participates has part of it to deliver your set of services as a company.

Harold Byun:

I think that there's going to be some significant consolidation in terms of what data actually leaves the boundaries. And there's other ways that you can start forcing vendors to come to you where you as an organization basically become the source of truth and the custodian of the data.

Harold Byun:

And one way to mitigate the risks around these third parties is to, quite frankly, not give them untethered access to that data. And so if you control that and consolidate the footprint of the data, then you're ultimately reducing your risks under some of these privacy regulation specifications.

Colin Whittaker:

Thank you very much indeed for that, Harold. And thank your [inaudible 00:57:56] for some of the resource implications. So I think we need to explore some of those a little bit more.

Colin Whittaker:

And we've got an audience panel, audience poll on that very issue now. And I'd like to remind my audience about the questions. And this one is trying to gather how much effort will be involved in responding to data such [inaudible 00:58:15] request, and what you currently estimate that to be.

Colin Whittaker:

So please feel free to respond to that question. And while you're doing so, I'm going to turn to Ilia. Ilia, once CCPA becomes effective, do you, yourself, screen the consumer requests for rightfully forgotten and more information people might have about them? And how do you think would be the best way to process them? And should organizations process all of them?

Ilia Sotnikov:

Yeah, that's a challenging question and thanks for that, Colin. So obviously, it's similar. Data subjects access rights are enforced by GDPR so we can learn from the experience that we see in UK or across the European Union.

Ilia Sotnikov:

And we see that this is not the same across the industry. So in different environments, companies that are dealing more with consumers and potential conflict resolution and things like that. So transportation companies, housing companies, that sort of companies, are dealing with potentially more of these access requests.

Ilia Sotnikov:

Specifically, not just because of the right to be forgotten, but because consumers found this as a new avenue to add pressure to their case when there is any sort of conflict.

Ilia Sotnikov:

So if you are in this B to C environment and if you are in one of those industries where you have seen historically more litigations and if you have been dealing with E-Discovery [inaudible 01:00:14] in more severe cases, E-Discovery requests based on the court orders or whatever, you can definitely expect to see a lot of those access requests. And you should plan resources accordingly.

Ilia Sotnikov:

And I think to the points that pretty much everyone on this panel already made and the previous poll showed that the biggest challenge seems to be around being prepared and mapping the data.

Ilia Sotnikov:

And not just within the systems of record. That would be nice and easy. But then your knowledge workers, your users are building the reports, doing the experts, sharing these types of data in presentations or Excel spreadsheets.

Ilia Sotnikov:

And then it can end up pretty much everywhere in Teams, in SharePoint online site. In a file share somewhere. In email somewhere. And all of that makes this more difficult.

Ilia Sotnikov:

So I'm looking at the poll results here as the audience is voting on this question on how much effort do they anticipate. And I see that a lot of, like almost two-thirds of the audience are going to invest to some extent. Whether thinking that this is going to be realistic or over the top.

Ilia Sotnikov:

So yeah, this will definitely require additional investment in the process and in the tooling to be able to map all the data, identify it and then be prepared for those requests as they come in.

Ilia Sotnikov:

And then I guess to the other aspect of your question, should you respond to all of them? That's another challenge because CCPA explicitly requires you to verify those requests. And there is not much guidance yet around what is the valid way to verify the requests and what you can use and what you can not use.

Ilia Sotnikov:

And that's definitely part of those comments on the final regulation that have been mentioned already. And that's definitely something that you should be looking into.

Ilia Sotnikov:

Understanding how you build that process, what kind of business units will be involved. What kind of roles and functions you will have in that process. Documenting it and then executing.

Colin Whittaker:

Thank you very much indeed, Ilia. That's a very useful lead in to one, Else. Because Else, earlier on you mentioned the importance of being able to answer these questions that come from the consumers in a way that can foster a good relationship with your customers. And if you don't, you get a bad relationship.

Colin Whittaker:

So how else can the CCPA be used as an opportunity to create a more powerful customer journey?

Dr. Else van der Berg:

Yeah, exactly. Thanks. So firstly, as I mentioned earlier, we've been talking to a lot of different businesses and we come across the same answer very often. Businesses seem to just want to get compliant and be done with all CCPA things.

Dr. Else van der Berg:

But on the other hand, I think what's important to realize, if you're already investing a large amount of money. And as K already painted way in the beginning, why not try to also get some ROI out of it? Apart from just avoiding the fines?

Dr. Else van der Berg:

Over the past months, we've actually seen multiple big techs like, for instance, Microsoft and Twitter come forward and really try to position themselves as pro-privacy advocates.

Dr. Else van der Berg:

I think that they don't do this only for altruistic motives. But that they actually know very well that it makes sense for them from a business perspective to build a very strong and trusting relationship with their customers. And put themselves forward in this way.

Dr. Else van der Berg:

Because I think that's the only way for them to come out on top in this day and age. So back to your question, how do you actually do it?

Dr. Else van der Berg:

So firstly, I'll go back to what I said in the beginning. It's really important that your entire customer journey, from beginning to end, is consistent. And also carries your tone of voice and your brand. So that's number one.

Dr. Else van der Berg:

Number two sounds very simple and a bit stupid. But it is quite important for your consumers that they are offered a very nice looking, uncluttered and modern interface that they can interact with.

Dr. Else van der Berg:

There was a study executed by a company called TechJury which found that 52% of users say that the reason why they don't return to a website is the way it looks. And 90% stopped using a service due to poor performance. So it's really, really important.

Dr. Else van der Berg:

And something that's always a CCPA requirement, by the way, is that you need to communicate with consumers in a transparent and honest way. In a way that gives them meaningful understanding about how their data is being handled.

Dr. Else van der Berg:

So that's how I think, in the end, this law is not only a cost, but also an opportunity that businesses should really seize.

Colin Whittaker:

Thank you very much indeed for that, Else. K, one of the questions people always ask is about tools. And we're going to have a panel, an audience poll question now about tools to support which is going to go live at the moment.

Colin Whittaker:

And while that's running and I encourage everyone to work out and provide their insight as what sort of tools that they think is most important.

Colin Whittaker:

But in your sense, you're a lawyer. What sort of tools and technology do you think will really help operationalize privacy from your perspective as being a lawyer.

Colin Whittaker:

Because generally speaking, people think it's cheaper to hire someone [inaudible 01:06:01] technology. But what's your view as a lawyer?

K. Royal:

My view is one, it's very difficult to hire someone that is skilled and has the expertise in the privacy laws that we're looking at. But two, complying with these laws is a lot bigger than having a privacy person. Yes, you need a privacy person that has skills and expertise.

K. Royal:

But even then, if your company is going to appropriately do its data inventory or mapping, for example. Or handle individual rights requests or consumer rights requests, you need tools in order to facilitate managing that appropriately, especially if you're going to get a lot.

K. Royal:

I mean one of the things that we saw under GDPR was people submitting or companies submitting. Who knows who was submitting fraudulent requests pertaining to consumers rights.

K. Royal:

And as you can imagine, that people who want to do bad, whether they're malicious actors or competitors could absolutely submit a request to you for consumers to be deleted that you have to spend your time to verify if that's an actual consumer and verify that it's the person that it is.

K. Royal:

But then to act upon it. So they could completely tie up your time and your efforts and your resources on busy work that you really don't want to be paying a skilled person by the hour in order to do work that tools could easily do for you.

K. Royal:

And looking at the responses coming in, I'm not surprised. So it looks like the biggest one so far is data inventory. Not surprised by that one at all and then consent. And I think I saw a question earlier about using cookie consent or browser options which is mentioned under the regulations.

K. Royal:

I do think that's going to be challenging. We don't know where the regulations are going to learn with using cookie consents or browser options in order to drive opting out of marketing.

K. Royal:

So I think tools in that area is going to be incredibly important. I love our audience. They're very highly intelligent.

Colin Whittaker:

Yeah, they're coming through with some good questions aren't they? Some really good ones.

K. Royal:

They absolutely are.

Colin Whittaker:

Yeah. I mean I agree with you. Having tools [inaudible 01:08:23] is important in trying to map out the flows within the organization is going to be critical to help improve this tooling a bit for the process in the future.

Colin Whittaker:

And actually, trying to map an account for the organization is going to be vital. The one thing I would say about consent and one thing that did give me concern is, of course, there's a double edged sword with a lot of it.

Colin Whittaker:

It's amazing how many phishing emails these days one's receiving which end up in spam, which purport to be from where one has actually to be forgotten. And asking if you really want to be forgotten.

Colin Whittaker:

And so that's a bit of a concern which the regulators weren't [inaudible 01:08:58] actually expecting it to come out to be targeted for ID based on new regulations coming out. So it's a bit of a shame.

Colin Whittaker:

Harold, can I turn to you finally before we go to the final takeaway. Really one of the questions about this is should organizations abandon any data monetization initiatives? Or are there compliant ways to collect information and then monetize it?

Harold Byun:

Yeah, I think it's, again, an interesting question. I think that it's going to be a challenge for a lot of organizations. My opinion is that the answer is no. I don't necessarily see people abandoning monetization policies.

Harold Byun:

I mean there's a lot of reasons for that. There's organizations that, quite frankly, just don't care. And there's also, on the flip side of it, when you look at revenue, there's obviously a lot of revenue to be gained through monetization.

Harold Byun:

And I mean there's classic examples of this with Facebook and other similar organizations that are collecting an incredible wealth of information and seemingly with disregard for any privacy aspects.

Harold Byun:

So I don't think that that is going to go away. I also don't think that the needs in the market are going to go away and on behalf of the consumer in terms of how people are engaging with technology and how information is delivered, whether that be through entertainment or health or exercise or whatever it may be.

Harold Byun:

There are a number of avenues where consumers are choosing to opt in. And so I think that this is an opportunity for organizations not only to comply and I think maybe it was Else who was talking about being a good citizen as it relates to data privacy.

Harold Byun:

But also look at ways that this could be extended into a competitive advantage. Because if you're struggling with the service requests, if you're struggling with mapping and you're struggling with the method of how you're actually going to execute on compliance, then you're not going to be able to execute successfully on a monetization strategy going forward.

Harold Byun:

And that's going to be a disadvantage for you from a business perspective. So I do think that organizations should continue to look at monetization strategies within the context of still remaining compliant. Within the context of ensuring confidentiality of the data. And looking at leveraging other means of methods to do this.

Harold Byun:

There are capabilities where organizations are looking to expose data as a service or data modeling as a service. And those types of things within the context of privacy regulations sound incredibly scary. But there are methods to facilitate that so that you're not completely throwing the baby out with the bath water, per se.

Colin Whittaker:

Thanks very much indeed for that, Harold. Well, thank you very much indeed to our panelists. There's some excellent discussion. And I know it's been appreciated by the audience. And certainly from the feedback we've been getting.

Colin Whittaker:

So we've come to the end. And I'm going to quickly go around the table and ask each of our panelists for their takeaway recommendation. Harold, you're first up so over to you. What was your takeaway for everyone please?

Harold Byun:

So I mean I think the takeaway is obviously get yourself educated much like you're doing today about what the privacy regulations and the impact to your business are going to be. And start looking at moving aggressively to implement the processes and procedures.

Harold Byun:

Because six months after the law goes into effect, that's when the Attorney General is going to stop suspending. I think they're giving you a six month grace period after January 1st.

Harold Byun:

And the revenue or the fine implications are obviously incredibly significant. And I think it's upwards of $750 per consumer record without actual viable cause that a consumer can actually file that grievance against your company.

Harold Byun:

So you definitely want to get things in order. There are more resources available. We have a white paper that's up here, but there's a Gartner report on the space. We have another webinar and deck on CCPA compliance mandates.

Harold Byun:

You can just go to baffle.io/CCPA and that'll take you to all the resources. Keep it simple and my emails as well.

Colin Whittaker:

Thank you very much.

Harold Byun:

Yep.

Colin Whittaker:

Thank you very much indeed, Harold. I'm sorry we have to move along. Else, what would be your final takeaway, recommendation to the audience tonight?

Dr. Else van der Berg:

Yeah, so I'm just looking through some of the votes from the audience in the polls and I'm just looking at this question about the data subject access requests. Whether they're ready. And it really stands out again that I see that 23% actually state that they believe that there will be more incoming requests than they can realistically handle.

Dr. Else van der Berg:

And I see a lot of people still investing in people and tools. Which is really interesting to see considering that the first of January deadline is really around the corner.

Dr. Else van der Berg:

And besides that, looking at all the questions that were asked. These are really, really interesting. As K also mentioned, they are also quite recognizable to me because I scanned through these comments. The comment period to the regulations.

Dr. Else van der Berg:

Looking at all of this, a lot of these questions actually are still open. Especially this question about these privacy settings in the browsers. These questions are still unclarified.

Dr. Else van der Berg:

So I think my key recommendation is, again, things are unsure and it does take a lot of time to actually get ready for the CCPA. So I think, again, don't try to do it alone. Don't try to tackle all of it in house. Try to outsource where possible.

Dr. Else van der Berg:

And on the other hand, something I've mentioned before, going for just the bare minimum of compliance will actually hurt your business because consumers will expect a very nice customer experience. And if you don't deliver that, it will damage your reputation as well.

Colin Whittaker:

Thank you, Else. Over to you, K.

K. Royal:

I have to agree with my co-panelists on the whole don't do it by yourself, reach out for help. All four of us here online and you can reach out to us. But I'm going to go a different direction then. I'm going to say that for companies who are based outside the US, my biggest takeaway is don't underestimate that ability for a private right of action or enforcement actions.

K. Royal:

The US and especially California is known to be very proactive in lawsuits and arguing the meaning of a single word. And enforcement actions. So please don't underestimate the impact of that and make sure that you're prepared for it.

Colin Whittaker:

Thank you very much indeed, K. Ilia, last word from you, thanks?

Ilia Sotnikov:

Sure. So I think it's all been said already, but my biggest takeaway from this, based on the questions, based on the votes, really you should know your data. You should understand what's going on, invest there and this will be the basis for everything else.

Ilia Sotnikov:

And then secondly, it is really important to see where you find the opportunities. So I think Else and K mentioned a lot of this, how you can change the culture. Building your relations with your customers.

Ilia Sotnikov:

But also on the IT operations side, make sure, understanding the data. Understanding the data flows. Understanding the processes opens tons of opportunities both in terms of saving the costs, getting rid of redundant data, et cetera. But also finding the opportunities, optimizing the processes, becoming more competitive. So find the ways to monetize this.

Colin Whittaker:

Thank you very much, Ilia. Over to you, Kelley, to close us out, please.

Kelley Vick:

All right, thank you, Colin. Thanks for a really good discussion everyone. And thank you to our attendees for your participation. Please do take a moment to leave us a rating and feedback. And be sure to scroll down to submit in your console. We value feedback and we take that into consideration when we're planning for future events.

Kelley Vick:

For those of you who follow for CPE credit, your certificate will be issued within 30 days. I'd like to remind those listening to check out our supporting resources and upcoming CPE programs related to today's topic by visiting executiveitforums.org where you can access our resources for free.

Kelley Vick:

Next month's CPE webinar is Cornerstones to Fortify Your Enterprise Cybersecurity Defense. And you can reserve your seat now through the console. So that's it for today. I'd like to thank our speakers for your participation with a special thanks to our sponsors, TrustArc, Datawallet, and Netwrix and Baffle without whom this event would not be possible.

Kelley Vick:

And, of course, thanks again for listening. Please stay tuned for our next event and Happy Holidays everyone.