Debaters:

Well done on getting through the round robin! I was pleased to see so many of you had done considerable research and prep. There is still time to improve your cases and get some additional background to help sell your arguments. The judges have taken time to write these emails with feedback so please read through them and then please remember to thank them for their time when you next see them.

Angela T.:

Remember the status quo: the IoT is here to stay and will continue to increase, as it does personal privacy will continue to be eroded. Every lay judge understand this to be the case. So in order to win a round on PRO you need to convince the judge that the benefits of continued growth of IoT far outweigh the risks of privacy loss…..To win on CON; you need to convince me that those benefits are not greater than my security or privacy loss.

Basically – if you are Pro – do not be afraid to say that you know there is currently a loss in PP but for the most part people are willingly giving that up – they would not do this unless they felt they were benefitting in other ways.

CON – use everyday examples that show we do not always have control or a choice in our privacy being “stolen” take the Target hack for example – millions of people who had shopped at Target had their credit card info stolen, it cost the store millions of dollars in lost revenues and it cost each individual time and money in ensuring they were not affected and then getting protection.

Pro – I liked the “improved quality of life” contention – give me more real life examples backed by data

In general, it seemed most of the novice teams I watched did not flow correctly and thus did not go through opponents arguments in an orderly manner. Also many were unsure what to cover and what not to cover in each of the speeches. Lastly, all teams both novice and returners had trouble with finding their cards quickly – I think significant work needs to be done on blocks to make it simpler to find the evidence card quickly.

Overall, PLEASE remember that you will be competing in front of mostly lay judges and that being the case you must appeal to them. Below is a discussion I had with Ryan with reagrds to the fact that some teams were running a non-topical contention on CON – (not related to privacy loss). He agrees it is not ideal and to be careful running it with lay judges:

Ryan Hartman:

CON: should the con side have any contentions that are non-topical, like Economy or Jobs?   
not optimal, to run an argument about economic harms. The idea behind it is this:

Neg really only has a few good arguments: (1) Privacy loss is bad because privacy has intrinsic value, (2) Cyberattacks are a form of privacy loss, cyberattacks are bad, (3) Corporations invade your privacy and store your info, creates security risks, (4) Privacy loss kills consumer confidence, which hurts the economy

I think all of those arguments are fine to bring up in the constructives, because they all use Privacy Loss as a link into their harms so they are still topical

A lot of our teams are running a big cybersecurity contention, but didn't want to run any of the other contentions on that list

So they decided to run the argument that internet of things automates labor, which kills jobs

**We decided to run that argument as a contention - even though it technically isn't topical offense for the neg - because it puts the affirmative in a really tough position**

i fear that with so many lay judges on the panel they will simply see it as non-topical

I think so too - I think it is much better to run the argument that privacy has intrinsic value and we should try to protect it as an important right

But the idea is the econ argument gets run as a time sink

Agreed!

It should be 30 seconds roughly to read, hopefully get the opponents to spend more time than that on it

Then, neg can just say "sure it isn't topical, but you just wasted a lot of time on it so now we're clearly winning other arguments"

I think it is much better to read the privacy is an important right argument, because it can be read in the same amount of time but will actually win the round if the opponents dont do a good job on it

problem is when the con team then spends too much time arguing a point that is not seen as topical and does not highlight the increase in privacy loss and lack of benefits

Yeah, I think that if con spends more time on the argument than the pro, it's a bad strategic decision for them

Judge 1:

PRO:

1. I feel the PRO side should be expanding their contentions beyond just Economy and Military (Saving Lives). I feel they should be strongly pushing the benefits of IoT: Increased efficiency (Cost Savings). Cars automatically moving forward at the same time (Saving gas), Far fewer accidents (Saving lives, saving money), Household automation (Fridges ordering food, identifying problems), Saving Electricity in the home and in the business, Safety and Security. Convenience to the user should also be something they can contend on.
2. I heard a couple of good one-liners: PRO: 'Con believes  that technology useful only if it is un-hackable'
3. The Pro side could actually concede that there will be an increase in hacking, but probably not much more than the current percentage. I do not know if this is true, but it sounds reasonable. This will allow them to say that IoT benefits everyone greatly (a rising tide lifts all boats), even if there is an increased in hacking

CON:

1. For a lay judge like myself, I could not understand the loss of jobs and income inequality in the constructive. These topics make sense negating the PRO Constructive during rebuttal but I don't think it should appear in the CON's constructive, since PRO could claim that it does not apply to privacy.
2. Privacy can be expanded to be more than just security. I liked the idea about insurance rates increasing (This is across the board, not just in Medical Insurance) because the Insurance Companies and monitoring their Fridges, Cars and Homes. I believe this can be linked to Privacy. Perhaps they can link the increased danger of connected devices to privacy
3. When talking about the impact of security breaches, a figure or 650 GB per second will mean nothing to most judges. However, quantifying the impact of real hacks (such as the ones at Target, Home Depot, and TJ Max to name a few) will have a greater impact. Do this in terms of people affected, cost of the outage and other costs such as folk now having to  pay for services to monitor their privacy and accounts - in effect exposing yourself even more if THESE companies are hacked, and they will be). For every instance of a hack, these values should be provided. Loss of income to those companies when people when it is unsafe to shop there.
4. Not one team mentioned the Jeep Hack (<https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>). This would be a great example to show.

Judge 2:

In general, the PRO cases missed on a couple of things:

1.        They didn’t address status quo—we already have essentially agreed to diminished privacy and tracking  when we buy smart devices and log onto the internet  – so IOT is not the culprit introducing this “new’ harm – we have already accepted this risk for the most part, and they could do a better job countering the incremental effect caused by new sources of data sharing/monitoring

2.       They didn’t really address technologies like add blockers and other filters that restrict sharing, monitoring and permissions to counter the con argument – if they shore this up, they could take away a very compelling argument from the other side

3.       They spent a lot of time on generic benefits (power grids, fuel savings) – but did very little to get me excited about IOT benefits for ME as a consumer.  If they are going to outweight the “harms” – these better be pretty good benefits and I just really didn’t hear benefits and impacts that were worth the privacy and security risks. Get more crisp on the benefits and quantification story.  This was challenged pretty rigorously in each round with varied effectiveness.

4.       Their narrative needs to get the other side to concede that “the horse is already out of the barn”….technology being integrated into our lives is here.  We can’t put that genie back in the bottle—and this trend will only continue at an increasing pace in the future.  Make the other side look old school.   Get the other side to concede that so far, things like smart devices and internet enabled services (some such as GPS navigation, e-commerce, On-star emergency monitoring & response, etc that rely on location and monitoring data) have already proven to be a net positive.  Would they want to give up their iphone and google maps in order to keep their location data private?

5.       Talk about lifestyle improvements – give compelling scenarios of what the future could be like, how our lives could be better/easier.  Give examples of how that has already happened in our lifetimes – share comfortable, supported and mainstream examples that are hard to refute.

6.       For crossfire:  a lot of con teams used “manipulative advertising” and monitoring as a key contention and harm.    Maybe pro should ask if consumers have “free will”  -- get con team to concede that just because we are monitored and served with tailored ads, it doesn’t mean that we are compelled to act on them.  Can they prove “harm” – or is this really just a satisfied consumer who got exactly what they wanted/needed more efficiently when they acted with free will?  Is this a harm – or really a benefit?

7.       The military application – combat cloud argument was generally weak.  Needs to be tightened up.  Con team was able to undercut most times by talking about exponential risk to centralizing military data which, if hacked, is more damaging – and that pro teams could not substantiate/win on security and encryption earlier arguments.

In general, the CON case missed on a couple of things:

1.       They also address big issues – security, privacy – but in big, general ways.  They could make these more personal by giving more real life examples of  privacy harms through situations where you would be “harmed”.  Only one team talked about car and health insurance rates being jacked up for specific people based on dietary habits derived from your IOT  refrigerator, or from driving habits reported by your IOT car monitors.  They also could show security harms through situations where monitoring companies (changes in electric usage, which lights are being used, if the alarm is on or off, etc…) to let hackers know when you are out of town (or home alone) – leaving you vulnerable and targetable for crime.

2.       In crossfire – it might be good to ask “how secure is secure enough” for IOT?....get the other side to concede that the security threshold of today is insufficient for the level of intrusion possible through IOT.  For example – how secure do you need your IOT in your car when you are on the roads?....do you want to be 80% sure that no one will hack your breaks or accelerator and be malicious?  How secure do you want your IOT pacemaker or medicine pump to be?.... you may be able to land the impact of personally invasive IOT and get them to concede, or at least fail to argue confidently in IOT encryption.

3.       Another thing that seemed a miss to me was that people weren’t really focusing in on the risk of hacking.  Hackers, by nature, really aren’t worried about or constrained by new IOT regulations and laws….because they don’t follow the rules.  How long does it take to hack into a system or release a destructive worm/virus?  Once it gets in one system – how easily can it spread to other systems and devices for mal-intended surveillance, monitoring,

4.       Also – on the vulnerability point, no one pointed to major hacks (DNC emails, State Department emails,  hacks into personal webcams of families, breeches of major retailers like Target, gas station card readers, major banks) – this is just a new reality – so to think IOTs would suffer any less of a fate seems to be missed.  Maybe some research/data on the prevalence of sophisticated corporate and government being disrupted and hacked would be important.

The pro rebuttal maybe could talk about “manipulative advertising” as a non-unique issue to IOT.  Advertising, by definition, is pitching products through various mediums (TV , radio, magazines, internet, coupons, direct mail, telemarketers, etc…) to targeted demographics.  So while they are not targeting a specific person – people are, and have been targeted by ads for decades.  Also- directed advertising is happening today on non-IOT devices (smart phones, laptops) – so even in a non-IOT world, this would still exist (albeit at maybe a lesser degree).  What evidence does the Con team have that personalized ads are bad and have “harms”?...

Also --  maybe give good examples of personalized marketing/ads….such as the safeway & QFC  advantage programs that track what you buy, and gives you relevant coupons for stuff you want/need  for future purchases, or lets you know when it’s on sale?....maybe find some other examples like this (airline loyalty programs with fare sales, etc)

**Judge 3:**

**Here are a few thoughts that I had after judging my round.**

**Of course, security and privacy was a big topic of discussion.  One of the items that the pro side mentioned but didn’t fully develop was the idea of the anonymizing of data.  If, wherever possible, a company can avoid collecting personal data, where it is not relevant or needed, then there really isn’t as much concern around privacy of the data.  That should have been a used more as a defense against privacy concerns.**

**The teams that I judged spent a lot of time debating whether traffic lights were part of the IoT.  Not every traffic light is hooked up to a network, but in the case of this topic, they should be talking about the ones that are hooked up to a smart grid system.  Don’t waste any time on this argument.**

**They could have drilled more into the loss of production jobs. While more STEM jobs would be created, more blue collar jobs would be lost.  Many blue collar workers would not be able to transfer over to STEM jobs and would therefore be potentially left without many opportunities**

Judge 4:

General feedback:

1. Prep before what rounds. We talked in our room about maybe not all kids know when you are allowed to prep. Fortunately I had my handy notes from you with me, so I was able to read to them verbatim, **They may take prep any time except just before cross-fires** – the kids in my group were pretty confident that wasn’t universally understood and that it would be beneficial to review this with the whole team.
2. Timing reminders – maybe take a pop quiz on what rounds are how long? Even the kids in my group – veterans – mis-remembered how long each round was and set their own timers for the wrong time. I had to call \***time**\* several times, and twice it was to their surprise. So a reminder would be good on memorizing the timing (again, so glad I had it plainly in front of me).
3. One of the suggestions I gave to the kids in my room was avoiding abusing jargon with a lay judge. “Non-topical” makes me think of medicine and isn’t an everyday part of my vocab. I understand it’s part of the debate vernacular, but to a lay judge, it sounds jarring to hear it every 10 seconds. I suggested finding other ways to make this point when faced with a lay judge, so it doesn’t come across as using the same word over and over. Maybe brainstorm other ways to make the same point (e.g., irrelevant).
4. The kids I had were very good, but even within that, there was a range in speaker presentation. Body language was something I took into effect, and used well, can suggest confidence and a superior position. Body language can also make you look frantic, disorganized, uncertain, etc. Not sure if this is something covered with the team but worth taking into consideration.
5. Eye contact. We discussed this in our judge training, and I noticed in my group of kids. I definitely noticed those who made regular eye contact with me – and opponents – versus staring at the wall or checking out the floor. I know this takes practice and a comfort level not everyone has, but it matters.
6. Demeanor – one of the boys in my group started giggling when someone else was talking. Frown. Also my son told me that his partner laughed in his debate as well. Unless it’s on purpose to make a point, lose the laughing.

Notes specifically regarding the case:

1. Technical jargon and acronyms. Because of the nature of the argument, technical jargon is necessary. But remember judges are not tech experts and so using too much jargon can come across like you’re talking over their head. I appreciated when an acronym was given what is stood for the first time it was used (just like you would when writing a paper). I appreciated when something technical was defined. But one time, one of my kids used a sentence with 3 acronyms that I wasn’t familiar with, and the following minute of argument was lost to me because I had no idea what he was talking about. It’s a balance, but there are definitely going to be judges who aren’t familiar with every term used in some of these memorized blurbs.
2. Employee productivity and automation was used too blurrily in my session as separate points. It was difficult to tell when one was arguing or defending one or the other. Either make them more distinct as separate arguments, or combine them to create a stronger argument, and pair with a different point.
3. A couple times, “technology” was seemingly interchangeably used with “internet” – for instance, a smart watch that will help me make burgers 10 seconds faster (?? Didn’t buy that one BTW). I don’t think everyone considers all pieces of technology as related to the internet – even if they sort of are, or one day might be… and that weakened the positions for me a little bit. Definitely didn’t add anything, so maybe just stick with things generally tied to the internet itself. OR – the flipside – make the case that everything is tied to the argument (but make the cases strongly) – e.g., even refrigerators have the ability now to order groceries for you, will we soon be used as data points for how many people have name brand soda in stock?
4. I LIKED the argument the CON side made about perpetuating income inequality – it was weakly correlated to the argument topic but I think if strengthened, would make a compelling point for the CON side with most judges.

Judge 5:

Just some ideas from yesterday's debate, in particular:

PRO-if CON argues loss of jobs due to automation, rebut as follows:

While this might be true for existing manufacturing facilities, whole new industries will be created.  Just look at South Lake Union. A whole new city is being created for blossoming technology that didn't even exist 10 years ago.  Those industries employ not only STEM folks but an army of support staff, sales, legal, HR, finance, and the list goes on.

Use real world examples - land line phones are becoming obsolete, so people who were employed to build phones in factories lose jobs.  But the creation of cell phones, builds entire new companies (Verizon, Sprint, etc.) and these new companies have new types of factories and employ millions. Add stats to bolster the argument.

PRO can rebut the above by arguing that IOT will force people previously working in hands on manufacturing into jobs they are not suited for and don't like.  Therefore, their quality of life will go down.

CON-argument about catastrophic cypersecurity breaches is rather weak - especially in absence of data.  There are many examples of cybersecurity breaches that have quantifiable economic ramifications.  Cite those examples showing real harm to the economy as a result of IOT (e.g., breach of security in a health insurance company, IRS, etc.)

PRO - good argument that IOT saves lives.  Focus specific examples again - fireman, soldiers with smart helmets, Compare deaths for a specific groups before and after implementation of IOT.

PRO - arguments on improved efficiency due to IOT are so grey and hard to quantify.

PRO-focus on real world healthcare examples. E.g., improved record keeping can help manage patient care across many facilities and doctors, decrease dangerous Rx interactions, etc. All of this saves money, time and improves quality of life for patients.

CON-tracking of shopping activities on web for marketing purposes is rather weak but one argument could go.  While may seem harmless and just a way for companies to make money, this is a form of personal espionage.  Companies can be using information to profile and make decisions that can affect credit scores, healthcare options, and insurance options, etc.  With IOT there is no way not to shop online or opt out of this personal espionage.  Only after the event has taken place, can the buyer decide to be unsubscribed from a list.  And then it's too late.

Judge 6:

The Pro side had a good case with strong impacts and was easy to relate to. Their Contention was Big Data with sub-points:

a. Health

b. Manufacturing

c. Business

d. Location

And the Con team had one Contention too,  Cybersecurity, with two sub- points:

a. High Security Risk

b. Corporate Security

Even though the Pro case was well presented and the case had better facts and impacts, the Con side did a better job at the summary, grand cross-fire, and final focus. Also, the Con side rebutted very well every single point to their opponent case and they still managed to defend their own case and argued their case better.