1 On Time Paragraphs

1.1 Paragraph
In “The Rise and Fall of Invasive ISP Surveillance,” Paul Ohm claims that Internet Service Providers “will continue aggressively to expand network monitoring” (p. 24). Though Ohm acknowledges that ISPs have “historically respected user privacy” (p. 5), he predicts that, without new regulations, “the inevitable result will be ISPs conducting full-packet capture of everything their users do” (p. 24). Ohm cites privacy breaches by Charter Communications and Comcast as examples of this “undeniable trend” (p. 18). However, backlash by lawmakers, advocacy groups, and the general public forced both Charter and Comcast to abandon their plans. Moreover, Ohm himself details how existing wiretapping laws already discourage ISPs from performing complete user surveillance (p. 65). Indeed, evidence suggests that Ohm’s predictions are not “inevitable,” and that the mere “potential” (p. 35) for privacy breaches does not necessitate sweeping new legislation after all.

1.2 Paragraph
A recent paper entitled “The Rise and Fall of Invasive ISP Surveillance” has caused a stir in the Duke Computer Science Department’s 182S class because of its strongly worded arguments and pretentious assumptions. Paul Ohm, the author of the paper, claims to have discovered a “grave...threat to privacy” in the Internet Service Provider (ISP). Comparing these ISP’s to wiretappers, Ohm claims that in the future the internet user will have no privacy unless strict legal measures are taken to prevent it. He goes on to explain that as the government made laws preventing the privacy of telephone users, so must the government begin to adhere to his advice and prevent ISP’s from encroaching on the privacy of the internet user. However, Paul Ohm’s reasoning is faulty and presumptuous. For one, he downplays the use of encryption to transfer information over the internet. He also simplified the origin of the privacy breach by saying it is more a problem of the ISP as opposed to holders of the information like Google.

1.3 Paragraph
Society’s ever increasing dependence on the internet has launched debates of online privacy to the forefront of academic research and discussion. While there has been much productive discourse on the topic, Paul Ohm’s “The Rise and Fall of Invasive ISP Surveillance” is only masquerading as academic research among other legitimate papers. Written from a first person perspective, Ohm
tirelessly places his own personal beliefs and predictions into the paper without substantive support. His arguments are repetitive and dependent upon embellished language to keep the reader’s interest - “imminent harm,” “the power to obliterate privacy online” and “a coming storm of unprecedented, invasive ISP monitoring” are just a few examples. Furthermore, Ohm’s paper offers no practical, executable suggestions in terms of policy changes that might protect user’s privacy and rights from the “dire harms” we all face in the near future because of the “unmistakable signs that things are getting worse.”

1.4 Paragraph

In today’s technological society, online privacy is certainly one of the biggest topics of concern to the billions of Internet users worldwide. Numerous magazine articles, newspaper columns, and academic papers have been written to voice their opinion or shed new light on this issue but one paper which falls drastically short in its accomplishing its purpose is Paul Ohm’s “The Rise and Fall of Invasive ISP Surveillance”. Beyond just the inappropriate title, which suggests that ISP surveillance is no longer an issue, Ohm writes his paper in a very sensationalistic manner not at all befitting of an academic paper but rather an opinionated editorial. Almost every sentence is heavily biased toward his opinion due to the overabundance of loaded diction that Ohm uses while the arguments he makes are flimsy and unsubstantiated from a lack of concrete evidence to support them. Much of the paper is filled with the words and ideas of others but in the cases that Ohm does push forth his own original ideas, there is a distinct lack of depth in his analysis and an almost arbitrary feel to how he draws his conclusions. If he were presenting his opinions in a column in some informal publication, a shortened version of this paper would certainly be appropriate, but for the realm of academia, this 83 page paper contains far too little academic substance and research to merit the consideration of any scholars reading it.

1.5 Paragraph

The Internet is undoubtedly one of the most revolutionary inventions of the modern world. It has become the fastest and in some ways the most efficient means of communication available to people today. Messages can be delivered from the U.S. to the Middle East in fractions of a second, and massive amounts of information are available to millions around the world on the world wide web. However, while the Internet has innumerable good uses, it is just as powerful when used for selfish motives. Therefore, those in control of the Internet are responsible for guiding the use of this technology in the right direction. In Paul Ohms paper The Rise and Fall of Invasive ISP Surveillance, he discusses the possibility of Internet Service Providers (ISPs) invading the privacy of users. Because all internet users must send and receive information from the internet through their ISP, the ISPs are in a unique position to watch anything and everything that is said, searched, and accessed online from any of their users. With the growing popularity of the Internet and the wide range of daily activities that are run through computers, the possibilities are frightening indeed.

1.6 Paragraph

The abstract for Paul Ohm’s paper, “The Rise and Fall of Invasive Surveillance” fulfills its basic roles as a decent abstract, but stops there. It lets readers know what the paper is about — the threat ISPs pose to internet privacy, how to deal with this threat, and how the privacy threat
ties in with the network neutrality debate. It also does a great job of establishing the others view point from the very beginning. It does this very forcefully in the opening sentence, where Ohm claims that, “Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP).” Though this is a very bold and hyperbolized statement, it is an effective first sentence of an abstract. It successfully catches readers attention, causing them to read me the exact point of an opening sentence. However, the abstract goes downhill from there. Ohm claims that, “This is only the leading edge of a coming storm of unprecedented and invasive ISP surveillance.” Again, Ohm makes a very powerful claim, but this time does it about predicting the future of internet privacy. Its hard to believe such an extreme statement about the future of the internet that has so many possibilities. Furthermore, Ohm offers no examples of what could be included in this “coming storm”. The combination of these causes Ohm to lose credibility as a researcher and author. Furthermore, Ohm goes on to make more intense, and now self-centered, comments on his thoughts on how ISPs threat to privacy plays in with network neutrality. He basically claims that while, “thousands of pages . . . have already been written about the topic, nobody has recognized” what he does about the network neutrality that already exists in “expansive wiretapping laws”. This statement does nothing to explain the contents of the paper, or the authors position on the topic. All it does is make the author seem arrogant, and does not belong in an abstract. Statements like these are what ultimately cause the abstractive to be ineffective. They cause potential readers to not want to read further into the paper, which is ultimately the goal of a good abstract.

1.7 Paragraph

Paul Ohms abstract to “The Rise and Fall of Invasive ISP Surveillance” is presented in a forceful and strongly opinionated manner. In just three paragraphs, Ohm introduces an eighty-two page paper that will argue the overwhelmingly dangerous power ISPs have over our personal online privacy. Using strong words and phrases, Ohm establishes a position of negativity toward the temptation that ISPs have to reveal our secret online lives to the rest of the world. What Ohm suggests as an innovative point that “nobody” has yet mentioned, however, is the expansive wiretapping laws that already exist which support network neutrality. In this brief summary, I think Ohm does a good job in presenting his concern over where online privacy is going today and the laws that have already been established to manage ISP invasion of online privacy. Although his words may sometimes seem overly opinionated and unnecessarily strong, Im interested in seeing if Ohm is able to support his forceful claims.

1.8 Paragraph

Do you ever feel like you are being watched? If you do, you are not alone. In The Rise and Fall of Invasive ISP Surveillance Paul Ohm talks about what he sees as the greatest threat to privacy society faces — ISPs. Although they are not currently storing any information about users, Ohm argues that recent technological advances, economic incentives and lack of “codified rules” for ethical practice will inevitably lead to invasion of privacy. This claim achieves its goal of attracting readers attention but loses its power if we consider some arguments that are never mentioned in the paper. First, moral principles exist even if they are not codified. Second, public outcry can and will influence potential attempt for invasion of privacy. Third, in a competitive market (such as the one for ISPs) if there is demand for an ISP that doesnt invade consumer privacy, such ISP will exist. Last, ISPs have had the means and incentives to invade our privacy for a long time. If
1.9  Paragraph

In an age where your broadband provider can see everything you do on the internet, anonymity and privacy might become a thing of the past. This issue is examined in Paul Ohm’s paper, “The Rise and Fall of Invasive ISP Surveillance”. Ohm contends that the Internet Service Provider (ISP) poses a greater threat to privacy than anything else in society. Since ISPs pose this type of threat to such a large group of people - a threat that has the potential to get worse - Ohm argues that ISPs must be regulated to improve user privacy.

1.10  Paragraph

There is a reason why people do not like lawyers. And this paper, “The Rise and Fall of Invasive ISP Surveillance” written by Paul Ohm, an Associate Law Professor at the University of Colorado Law School, is no exception. Paul Ohm starts off in his Abstract: “Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP) (1).” He makes it sound like the ISPs have control of everything and as if this “potential” problem cannot be easily fixed. He makes this seem worse than it needs to be. Policymakers just have to follow the basic telecommunications privacy. Therefore there is no need to balance “between an ISP’s legitimate needs and mere desires” because then the ISPs will just want more invasive power which will just cause issues. Dr. Ohm also claims that these policies he is going to lay out will “help inject” privacy into the network neutrality debate, which has already been in discussion, so it is nothing new. He does not stop there, he continues by saying that understanding the idea will “flip the status quo” which does not make any sense. The paper starts off with short Abstract to briefly outline what the paper is about, but his topics seem weak and makes this topic seem worse than it actually is.

1.11  Paragraph

Paul Ohm argues that is illegal to use deep packet inspection (DPI) to monitor the contents of packets before they are sent to the user. He also concedes that “ISPs face no civil liability for non-content monitoring.” This means that under current law, network neutrality is maintained only because it is illegal for ISPs to look in the contents of the packets. However, it is possible to violate network neutrality without using DPI. If an ISP were to look at the source of the header of each packet and deliberately slow down delivery of packets that came from certain sources, then the network is no longer neutral, even though the privacy of the user is maintained.

1.12  Paragraph

The rise of the internet has caused a new legal interest in issues of communications technologies that have been long thought settled; among the most important of these issues is whether the provider of a communications technology may freely access and use the communications it transmits. This issue is taken up by Paul Ohm in “The Rise and Fall of Invasive ISP Surveillance,” a forceful paper warning of great dangers in internet service providers’ (ISPs’) surveillance of their users’ internet communications. Ohm’s paper is long—over 80 pages—but its abstract makes extremely strong claims that, if fulfilled, would justify the length. He claims ISP surveillance to be the greatest risk
to privacy in all of society, thus surpassing all governmental, criminal, and offline activity. He also presents the legality of ISP surveillance as crucial to the net neutrality debate. In fact, he claims that this paper completely transforms that debate by revealing that net neutrality is required by existing anti-wiretapping regulations and by recasting privacy as the central issue in that debate. Ohm continues to make powerful claims throughout the paper. He states on p. 24 that the ethics of ISP surveillance are and always have been poorly defined. This is a valid point; there is indeed little consensus on the ethics of this issue. While such a claim about ethics would tend to incite debate, the debate itself would affirm the claim by showing the lack of consensus. In all, Ohm’s paper is characterized by very strong claims, some of which show significant merit; some, for example that “a neutral network is a more private network” (p. 81), likely go too far and suggest that Ohm may have overextended himself in the forcefulness of his abstract, but the paper should not be dismissed as overly arrogant without paying attention to its contributions.

1.13 Paragraph

After reading the title of this paper, I expected that I would be reading 83 pages recounting the history of ISP surveillance and how it no longer poses a threat. That changed, however, when I read the first sentence of the abstract — “Nothing in society poses as grave a threat to privacy as the Internet Service Provider.” While this sensationalist claim is supposed to draw the reader in and compel them to read on, I found it laughable. After reading more of the paper, I found the premise on which Ohm bases his argument on to be weak — he claims that ISPs pose a grave threat to users but then mentions have in the past they have respected user privacy. He claims that because technology is evolving, ISPs will now fail to respect said privacy. He fails to convey the legitimacy of this threat — just because the technology is available, why would ISPs suddenly change their policies and infringe on user privacy. There must have been something other than a lack of technology that was preventing them from such infringements, like a business strategy or something written into the ISPs policy.

1.14 Paragraph

Paul Ohm, in his paper “The Rise and Fall of Invasive ISP Surveillance,” argues that Internet Service Providers like a common set of established rules regarding user privacy and security. After citing numerous examples of unsatisfactory privacy policies and invasive behavior, Ohm attempts to increase the awareness of his plight by comparing it to the current debate over network neutrality, hoping to leverage some of the widely-publicized disputes notoriety. However, much of his work is based on broad, polarized claims that can be easily discredited with straightforward examples. In this manner, it will demonstrated that Ohms views are not representative of the current state of ISP surveillance and privacy is an issue separate from network neutrality.

1.15 Paragraph

“The Rise and Fall of Invasive ISP Surveillance” by Paul Ohm is an incomplete argument in its technical, ethic, and political aspects. His emotive phrases and claims are not well-supported by the arguments in the paper. When explaining actions taken by ISPs for example, he says “though the technical details are still murky...”. He also overplays the role that wiretapping laws play in network neutrality. Like this paragraph, he needs more content and supporting statements to make
Ohm’s commentary on the ethics of Comcast’s approach toward BitTorrent traffic and the danger of ISP control over networks suffers from an inane lack of clear thought. After a summary of Comcast’s activities in which he highlights the FCC’s legal reprimand of the company, Ohm asks whether the acts of ISPs he has explained are ethical. With an answer to this question nowhere to be found, instead he mentions criticism of the company and the fact that providers often put spin on their actions through some sort of public relations effort and concludes that ethics are simply not “well-delineated” in network monitoring. Finally, despite having noted Comcast’s failure to continue monitoring as before in light of the FCC as well as having said little to nothing about what role ethics plays in restraining companies, his train of thought continues without hesitation to the marvelous conclusion that “the inevitable result will be ISPs conducting full-packet capture of everything their users do”. This chain of reasoning in reality is a stream of disconnected thoughts which overwhelm the reader with nominal evidence while Ohm evinces his own inferences as firmly derived; Ohm does little to build a good argument and substitutes content for substance.

The Internet is undoubtedly one of the most revolutionary inventions of the modern world. It has become the fastest and in some ways the most efficient means of communication available to people today. Messages can be delivered from the U.S. to the Middle East in fractions of a second, and massive amounts of information are available to millions around the world on the world wide web. However, while the Internet has innumerable good uses, it is just as powerful when used for selfish motives. Therefore, those in control of the Internet are responsible for guiding the use of this technology in the right direction. In Paul Ohms paper The Rise and Fall of Invasive ISP Surveillance, he discusses the possibility of Internet Service Providers (ISPs) invading the privacy of users. Because all internet users must send and receive information from the internet through their ISP, the ISPs are in a unique position to watch anything and everything that is said, searched, and accessed online from any of their users. With the growing popularity of the Internet and the wide range of daily activities that are run through computers, the possibilities are frightening indeed.

In “The Rise and Fall of Invasive ISP Surveillance” Paul Ohm paints a dreary and dismal picture of the future of internet privacy. Using sensational and at times over zealous phrasing Ohm attempts to shed light on a precarious situation of internet service providers (ISPs) “aggressively monitoring” and “spying” on client packages. While Ohms fundamental concern with the increasing need for wide sweeping and unambiguous policy concerning ISP-client privacy is quite founded, the degree to which he stresses the nature of the situation is a bit fanatical. In the abstract Ohm claims that his article “refines earlier theories of communications privacy to help policymakers strike the proper balance between user privacy and ISP need.” Despite his fervor Ohm did very little to add original ideas to the subject at hand, to provide multiple concrete examples of invasive ISP practices, and
to give thorough tangible and flexible solutions. One of the main counter arguments to his claim is the understanding that in general people will adamantly oppose a very intrusive ISP and will either seek service elsewhere or will demand legislation that strictly upholds their right to privacy.

2.2 Paragraph

I originally tried to read Paul Ohm’s article “The Rise and Fall of Invasive ISP Surveillance” with an open mind, in spite of his incredibly audacious claims. A look at the table of contents of this 82 page article will tell you that he has put a lot of time into writing this. And one can agree that there is a potential threat to privacy from ISP’s, so his charismatic style makes you curious if he can back his claims up: statements such as Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP). and “This is only the leading edge of a coming storm of unprecedented and invasive ISP surveillance.” and “The recognition of this idea will flip the status quo and reinvigorate a stagnant debate by introducing privacy and personal autonomy into a discussion that has only ever been about economics and innovation.”, all of which came only from the abstract. But after doing some reading and thinking for myself, I have found that though he recognizes some potential problems, and gives some good points, his ideas are not at all original. They are certainly not going to “flip the status quo” or reinvigorate anything. The information is good and it is convenient that he has collected these arguments and ideas into one place, but they are not profound or new, and some of his arguments and statements are flawed. I will attempt to address of few of his main points.